役員による役員のためのガイド

Cybersecurity: 取締役会のための7つのステップ

効果的なサイバーリスク管理の手引き

BY **ANDY BROWN & HELMUTH LUDWIG**

2023年10月初版発行
ISBN Number: 979-8-9871864-8-0

Cybersecurity: 取締役会のための7つのステップ

役員による役員のためのガイド:
効果的なサイバーリスク管理の手引き

BY **ANDY BROWN & HELMUTH LUDWIG**

著者紹介

アンディ・ブラウンは、エンタープライズSaaS、セキュリティ、AI企業の構築に焦点を当てたアドバイザリー会社、Sand Hill EastのCEO兼創設者。現在、Zscaler、Pure Storage、Digital Asset、Skyhiveなどのテクノロジー企業の取締役を務める。彼は30年以上の経験を持つベテランの企業技術幹部である。

大手企業でセキュアなデジタルトランスフォーメーションをリードしてきた30年以上の経験を持つ。UBSのグループCTO、Bank of America Merrill Lynchの戦略・アーキテクチャー・最適化部門責任者、Credit Suisseのインフラストラクチャ部門CTOを経て、Merrill Lynch、Paribas、BT、シェル石油で数多くの職務を歴任。

ヘルムス・ルドウィグはSMUダラス校コックス・スクール・オブ・ビジネス教授。現在、日立製作所東京本社、 Circor International（会長）、Humanetics Group（会長）など複数の産業企業の取締役を務める。また、Bridgepoint LLCのシニア・アドバイザーであり、Siemensの元グローバルCIOでもある。CIOとして在任中、ITチームはユーザー重視の非常に革新的なビジネス・イネーブラーへと変貌を遂げた。この変革が評価され、2019年に名誉あるCIO賞を受賞。

その他の協力者

ローレン・ワイズ – Zscaler グローバルエグゼクティブアドバイザリー担当シニアディレクター
ダニエル・バルマー – Zscaler シニアトランスフォーメーションアナリスト
サンジット・ガングリ - Zscaler CTO・イン・レジデンス

序文

デイヴィッド・G・デウォルト

『サイバーセキュリティ: 取締役会のための7つのステップ』へようこそ。サイバーセキュリティの世界と、今日のデジタル環境におけるその意義についてご紹介できることを光栄に思います。私は、サイバーセキュリティ、セーフティ、セキュリティ、プライバシー市場に特化したベンチャーキャピタルNightDragonの創業者兼CEOであり、FireEye、McAfee、Documentumの元CEOであるデイブ・デウォルトです。また、大統領の国家安全保障電気通信諮問委員会（NSTAC）のメンバーであり、CISAサイバーセキュリティ諮問委員会（CSAC）の副委員長でもあります。

私は経験豊富なサイバーセキュリティ・リーダーであり、組織、政府、重要インフラがデジタル資産の安全を確保するにあたり直面する課題を深く理解する役員でもあります。本書では、アンディとヘルムスが、実務家として、また取締役会メンバーとして、サイバーセキュリティの複雑な領域を切り抜けてゆく他の取締役を支援するために、彼らの生きた知識と専門知識を共有しています。私と同様、アンディとヘルムスもサイバーセキュリティの分野では高い評価を得ています。

近年、さまざまな業界の組織を標的としたサイバー攻撃が急増しています。よく知られたデータ漏洩事件からランサムウェア攻撃まで、これらの事件は、強固なサイバーセキュリティ対策の重要性を浮き彫りにしています。本書では、サイバー攻撃の実例とその結末を探り、進化する脅威の状況や採用可能な防御戦略に関する貴重な洞察を提供します。

最高レベルの監督機関である取締役会のメンバーは、組織内で効果的なサイバーセキュリティを実現する上で極めて重要な役割を果たします。取締役会のメンバーは、サイバーセキュリティ方針の議論や意思決定プロセスに積極的に関与することで、組織におけるセキュリティとレジリエンスの習慣を確立し、増大するサイバーリスクを軽減するための最善の準備を整えることができます。本書は、取締役会のメンバーが、組織内だけでなく、業界内のより広い範囲で積極的なサイバーセキュリティ推進者になるための道しるべとなるでしょう。

私はこれまでのキャリアを通じて、何千件ものインシデントへの対応活動を指揮する中で、サイバー攻撃が個人や組織に与える壊滅的な影響を目の当たりにしてきました。このような経験から、私は、取締役会やその他の経営幹部に対して、サイバーセキュリティに関する継続的な教育と啓発の必要性を強く感じています。

『サイバーセキュリティ: 取締役会のための7つのステップ』が、組織のサイバーセキュリティ対策を強化しようとする取締役会メンバーにとって貴重なリソースとなることを願っています。共に、より安全なデジタルの未来に向けた旅に出ようではありませんか。

デイヴィッド・G・デウォルト

目次

はじめに

サイバーセキュリティは、規模の大小や上場・非上場を問わず、すべての企業にとってミッション・クリティカル（業務遂行に必要不可欠な要素）であり、取締役会には、組織が十分に保護されていることを保証する受託者責任があります。そこで我々は、セキュリティ変革の道のりの手引きとなるよう、リスク管理のためのサイバーセキュリティの主要トピックを網羅した、取締役会に関係する7つのステップによるプロセスを構築しました。
取締役会の一員としてのあなたの役割は、エンタープライズリスク（サイバーリスクだけでなく、事業リスク、信用リスク、市場リスクなども含む）を監督することにあります。サイバーリスクを管理するには、なぜ組織がサイバー攻撃の危険に晒されるのか、基本的な要因を理解する必要があります。

法規制、技術的な課題、組織文化、ビジネスパートナーシップのすべてが、組織のサイバーリスクに直接影響します。本書では、組織のサイバーリスクを評価、管理、改善する際に考慮すべき様々な要素を包括的に取り上げました。

サイバーセキュリティは、これまではリスク管理の一要素に過ぎなかったかもしれませんが、発生の確率と影響の大きさの両面で、重要なリスクにランクアップしています。サイバー攻撃はあらゆる場所で発生するようになっただけでなく、大きな風評被害に加え、深刻な金銭的損失をもたらしています。

「人を騙すのは、すでに騙されたことを納得させるより簡単だ」

マーク・トゥエイン

取締役の善管注意義務

Caremark1判決は、Caremarkドクトリンとも呼ばれ、企業のコンプライアンスとリスク管理の監督に関する会社取締役の責任を定めた法的基準です。同判決は、取締役に対し、法や規制の遵守を監督し、対処するための内部統制システムおよび報告の仕組みを確立し、維持することを求めています。

この法律は、取締役サイバーリスクの監督分野において負う義務について言及しており、(1)取締役会がサイバー管理システムの導入を「完全に怠った」かどうか、または(2)取締役会が意識的または故意に危険の兆候への対応やそのシステム内での責任の遂行を怠ったかどうかを判断することができます。

取締役会の不作為にCaremark法を適用しようとする最近の試みは否定されましたが、これは変わるかもしれません。サイバートランスペアレンシー（サイバーセキュリティに関する透明性）に関する法規制が厳しくなり、サイバーインシデントの影響が増大し、時には世界的大規模なものとなっているため、将来的に取締役会が責任を負う可能性は高まっています。

サイバーリスクは3つの領域で評価することができます:

- 組織が許容できるリスク量（許容可能な損失の量）
- サイバー保険によって第三者に転嫁できるリスク量
- サイバーセキュリティ技術やトレーニングなどへの投資によって軽減し得るリスク量

本書は主にリスク軽減における取締役会の役割に焦点を当てていますが、取締役会の一員であるあなたも、許容可能な損失の量を決定し、リスク転嫁戦略を策定する上で重要な役割を果たします。

1 1996年の米国デラウェア州裁判所での画期的な事例として、チャンセリー裁判所によって判示されたケアマーク事例の判決は、取締役会の監視活動義務を明確にした。

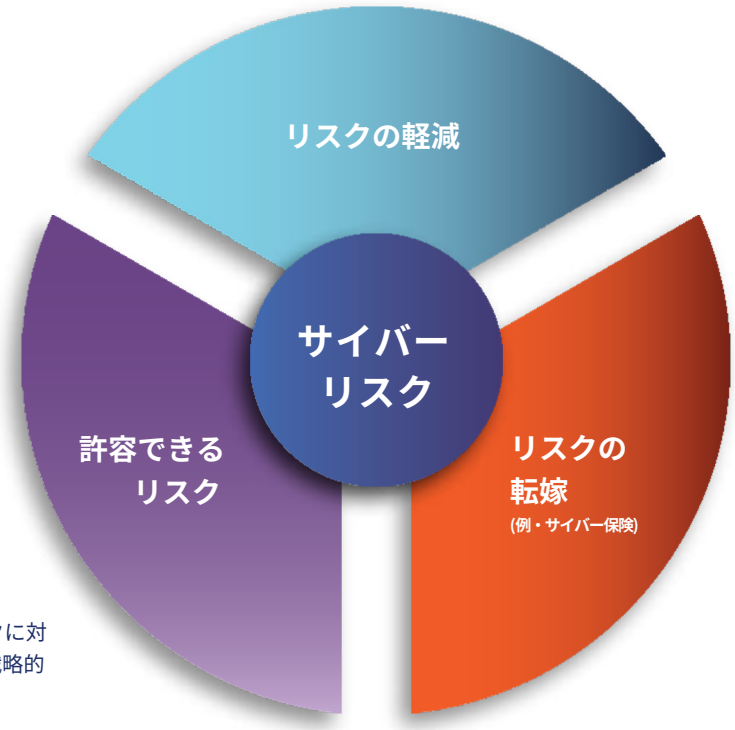


図01：サイバーリスクに対処する際、組織には戦略的オプションがある。

今日、取締役は、自組織のサイバーリスクとサイバーセキュリティ対策の現状に関する知識と理解を深め、経営陣が行動を起こすよう積極的に働きかける必要があります。

我々はどのようにしてここまで来たのか？

情報技術、そして組織が競争力を維持するためにそれを利用する必要性は、時代とともに複雑さを増しています。サイバーセキュリティも同様に、従業員、アプリケーション、データが分散した企業の保護を追い求める中で、より複雑になっています。エンドユーザー・コンピューティング、クラウド、データセンターなどのテクノロジーが、資産を保護するためのファイアウォール、プロキシサーバー、データ損失防止エンジンと共に主要な焦点となるようになりました。

このような進展により、最高情報セキュリティ責任者（CISO）という、ますます重要性を増す指導的役割が登場しました。CISOの最終的な責任は、組織の人材、コンピュータ・ハードウェア、ソフトウェア、情報資産を保護し、ポリシーを設定することです。このようにセキュリティに特化することで、CISOの役割はIT部門やその他の経営陣、取締役会から切り離されるようになりました。

2007年以降、クラウドの登場とともにテクノロジーの進化のペースは加速しました。市場シェアやマーケットの投資先は、徐々に社内のデータセンターから、Amazon Web Services（AWS）、Google Cloud Platform（GCP）、MicrosoftのAzureといったIaaS（Infrastructure as a Service）ベンダーへと移っていきました。それと同時に、Microsoft、Google、Salesforce、Workday、Zoomなどの企業がSaaS（Software as a Service）プラットフォームでのサービスを提供し始めました。

価格、市場投入までの時間、開発者の生産性、そして巨大なコンピューティング能力を活用できることがクラウド採用の最大の原動力となりました。これにより、企業は市場での競争優位性を獲得しましたが、その結果、データは、データセンター、IaaS/SaaSソリューション・プロバイダー、複数の地理的な場所に分散することになりました。

サイバーセキュリティの観点からは、データはどこにあっても保護されなければならないため、これは大きな組織的リスクとなります。また、多くのクラウドサービスやプラットフォームは、データ共有機能を備えており、その実行も必要となります。従来のネットワーク・アーキテクチャーやセキュリティ・アーキテクチャーは、この新たな世界でサイバーリスクを管理するのに十分な速さで進化していませんでした。

その結果、新しい技術の進歩に起因する侵害や情報漏洩が何件も公になり、大きな話題となりました。その中には、元UberのCISOであるジョセフ・サリバン氏が起訴される[2]など、企業への強制捜査につながったものもあります[3]。SECによる同様の動きは、2020年の情報漏えい事件後、SolarWindsのCISOに対しても行われています[4]。今日、複雑なセキュリティ問題に対する法的責任は、業界全体、特にCISOや取締役会に大きな動揺と不安を与えています。SECは、2023年7月、サイバー侵害が発生した場合に求められることを正式に規定する裁定を下しました。

2 2016年にUber Technologies社で発生したハッキングによる情報漏洩について、当時最高セキュリティ責任者であったジョセフ・サリバン氏が情報隠蔽を指示し、3年間の保護観察期間と罰金5万ドルの支払いが命じられた。
3 (2023, May 5). Uber's Ex-Security Chief Leaves Court With No Jail for Covering Up Massive Hack. Gizmodo. https://gizmodo.com/uber-security-joe-sullivan-sentenced-prison-data-breach-1850403347
4 SECは、SolarWinds社と最高情報セキュリティ責任者 ティモシー・G・ブラウン氏を、既知のサイバーセキュリティリスクと脆弱（ぜいじゃく）性に関連する詐欺行為および内部統制の不備で告発した。

SECによるサイバー情報開示規則

2023年7月26日、SECはサイバーセキュリティに関する裁定[5]を下し、公開企業に対して以下の内容を義務付けました（移行期間後）：

- 重要と判断されたサイバーセキュリティ・インシデントに関する情報開示
- インシデントの性質、範囲、時期に関する重要な側面についての説明
- 会社に与える重大な影響、またはその可能性のある重大な影響の開示

これは、発生したサイバーセキュリティ・インシデントが重大なものであると企業が判断してから4営業日後が期限となりますが、国家安全保障または公共の安全に対する実質的なリスクがある場合は期限を延期することが可能です。これは米国司法長官によって決定されます。
加えて、この裁定では、重大なサイバーリスクの評価と管理に責任を持つ企業経営陣の関連した専門知識の開示を要求しています。さらに、この規則では、重大なサイバーセキュリティ リスクを評価、特定、管理するための企業のプロセスについて、経営陣の役割と取締役会による監督の両方を含む定期的な開示を要求しています。

リスクへの露出に対する理解の必要性、 投資の抑策策、完了までのタイムスケールは、取締役会の議題の必須トピックとなっています。サイバー対策に先進的な一部の取締役会では、サイバーリスクの監督がより正式に行われるようになっており、サイバーリスクや、より広範なリスク管理に特化した専門の監査委員会やタスクフォースを設置する企業もあります。これらの委員会には、テクノロジー、リスク管理、またはサイバーセキュリティの専門知識を有する取締役会メンバーや、サイバーセキュリティ・コンサルタントや法律専門家などの外部アドバイザーが含まれ、プロセスの成熟度評価を担当する場合もあります。

5 SEC (2023, July 26). Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

CISOとの役割分担のバランスを取るため、組織によっては、セキュリティポリシーを担当する最高リスク責任者（CRO）が存在することもあります。CRO または CISO の役割は、サイバーセキュリティ・ポリシーを施行することです。取締役会のメンバーは、社内の特別な役職（CISO や CROなど）に、組織内部のレポートラインと取締役会委員会へ直通のレポートラインを確保する責任を負います。通常、CISO/CROは四半期ごとに監査委員会に最新情報を提供し、CIOは年1回、取締役会全体に最新情報を提供します。

さらに、組織の内部監査部門やコンプライアンス（法務）部門もサイバーリスク管理の手助けとなります。これらの部門は、会社がサイバー関連の法律や規制の要件を遵守していることを確認し、会社の内部統制におけるリスクや弱点を特定することができます。

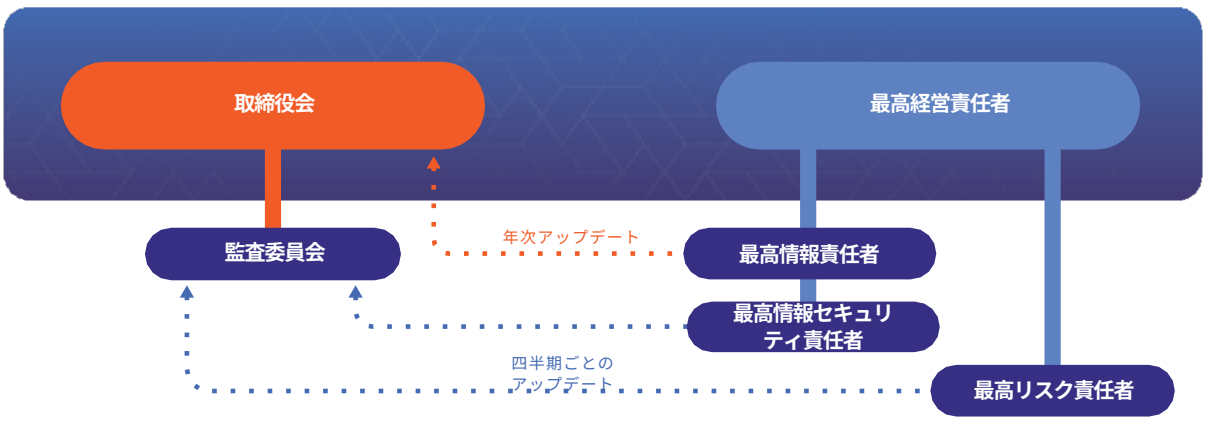
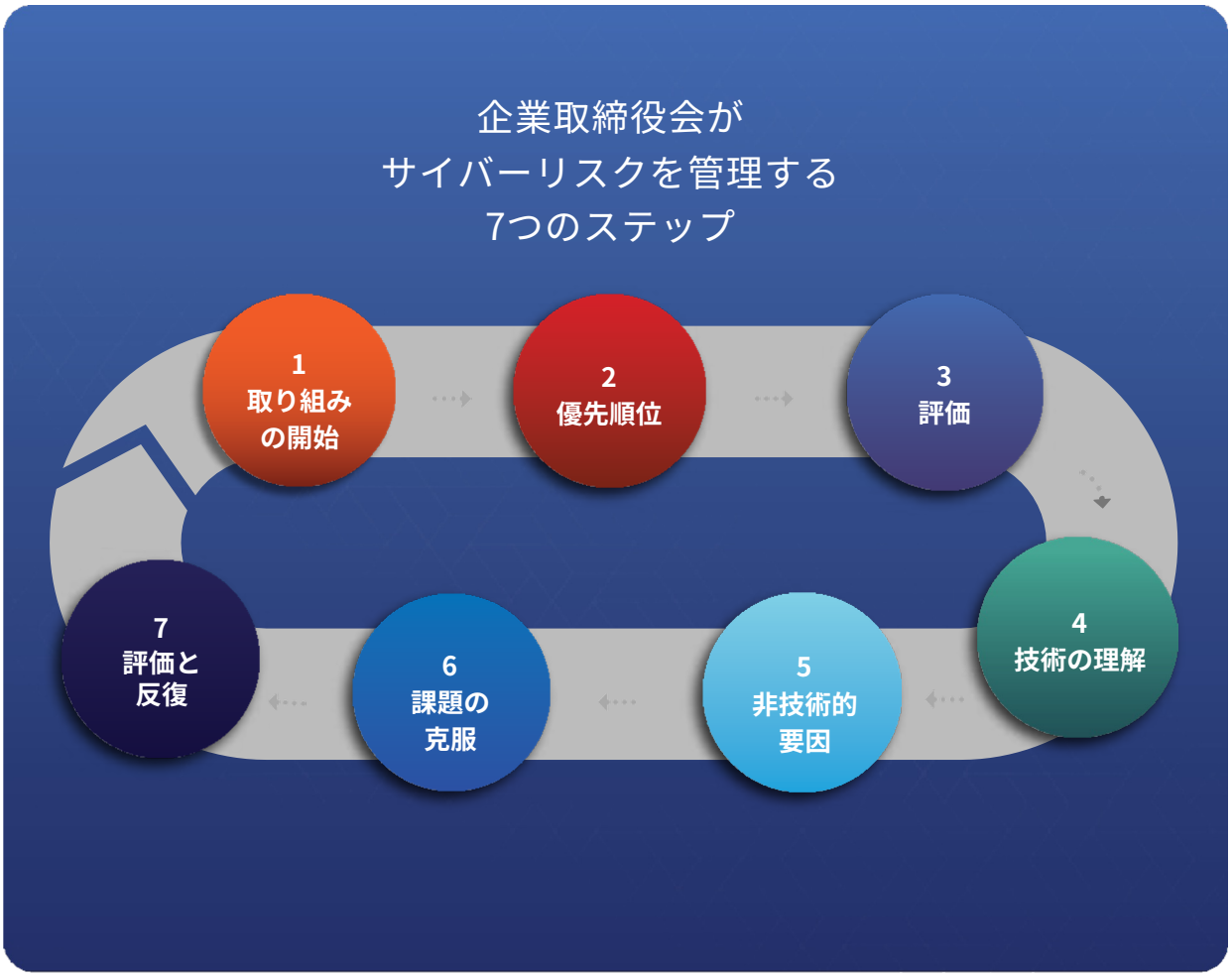


図02：取締役会と経営幹部の機能的関係

このような背景を踏まえた上で、組織のサイバーリスク管理を成功させるためにはどのようにすればよいでしょうか。本書では、その答えを7つのステップに分け、優れたリスク軽減が実証されているゼロトラスト・アーキテクチャーの有望性について詳しく説明します。ゼロトラスト・アーキテクチャーはリスク軽減に加え、ユーザビリティを向上させ、技術コストを削減します。


企業取締役会が
サイバーリスクを管理する
7つのステップ
1
取り組み
の開始
2
優先順位
3
評価
4
技術の理解
5
非技術的
要因
6
課題の
克服
7
評価と
反復

取り組みを始めるには

サイバーリスク管理における取締役会の役割

なぜこのステップが重要なのか？

取締役会は、組織がサイバーリスク管理を行う上で主要な役割を果たします。テクノロジーは常に変化し続けるため、サイバーリスク管理の取り組みは、時間をかけ、継続的に改善していかなければなりません。システムに対するサイバーセキュリティのギャップや、セキュリティの脆弱性は、規制リスク、刑事リスク、法的リスク、ブランドリスクを引き起こす可能性があり、取締役会はそれらのリスクを理解し、監督する必要があります。今も世界のどこかで、サイバー犯罪者があなたの組織への攻撃を計画し、知的財産や競合情報、または詐欺や恐喝に利用できる情報を狙っているかもしれないのです。サイバーリスクに焦点を当て、業務および財務への影響に関する透明性の高い報告を受けることで、取締役会は、組織がさらされているテクノロジーに起因するリスクをより明確に理解することができます。

取締役会は何をすべきか？

データとITシステムの管理とガバナンスにおいて、あなたの役割は組織の成功に大きく関わります。まずは、組織の技術的な能力とプロセスについて基本的な理解を深めましょう。これにより、十分な情報に基づいて、サイバーセキュリティへの投資の優先順位付けし、適切に配分を行うことができます。また、サイバー攻撃に関連する法律や規制の枠組みについても詳しく学ぶことで、よりリスク管理を行いやすくなります。

投資の支出レベルや相対的な優先順位を設定する際には、組織がどの程度リスクにさらされているかを検証し、リスク管理体制を評価します。より広範なリスク管理計画の一部としてサイバーセキュリティに焦点を当てましょう。組織が適切に保護され、準備されていることを確実に

サイバーセキュリティのギャップや脆弱性は、規制リスク、刑事リスク、法的リスク、ブランドリスクを生み出し、そのすべてを取締役会が理解し、監督する必要があります。

するためには、大規模なサイバーインシデントが発生する前に、あなたがサイバーセキュリティに関する自身の役割を果たしている必要があります。「インシデントが発生してから関与すればいい」と考える人はいないはずです。組織のサイバーリスクを軽減するためには、攻撃を受ける前に実施しておくべき効果的な対策があります。

大規模なサイバーインシデントが発生した際に、会社、顧客、従業員、株主にとって役立つ予防策を今から検討しておきましょう。

- 経営陣、リーダーシップ、取締役会の立場から、サイバーリスクに対する直接的な責任があることを明確にする。
- 各インシデントがどのように対処され、伝達されるかを把握する。
- 実際のインシデントをシミュレーションすることで、セキュリティインシデ ント対策の演習とテストが実施されていることを確認する。

CEOは会社の成功に対して最終的な責任を負っており、その中にはサイバーリスクの管理も含まれます。CEOは、CROやCISOなどの重要な役職に特定の責務を委任することができますが、サイバーリスクは組織のどの部分からも発生する可能性があるため、他にも組織的なサポートが必要です。すべてのチームメンバーがサイバーセキュリティのリスクを認識し、十分なトレーニングを受ける文化を作りましょう。

取締役会の役割は、事業が安全に遂行できるようにリスクを管理することです。サイバーセキュリティは、取締役会に関わるすべてのリスク領域に関係性があり、サイバーリスク管理をどう行うかは、組織の成長から安定性まで、すべてに影響を与えます。サイバー脅威は、組織の評判に影響を与えたり、地政学的な影響を及ぼすだけでなく、法律や規制に関する問題を引き起こす可能性もあります。リスク管理の枠組みや方針を統括する取締役会は、サイバーリスクを含むリスク管理の内部統制を維持する責任を負っています。

また、取締役会のメンバーにサイバーセキュリティの専門家を置き、セキュリティとリスクの基本的な考え方をしっかりと理解することが求められていくことも予想されます。

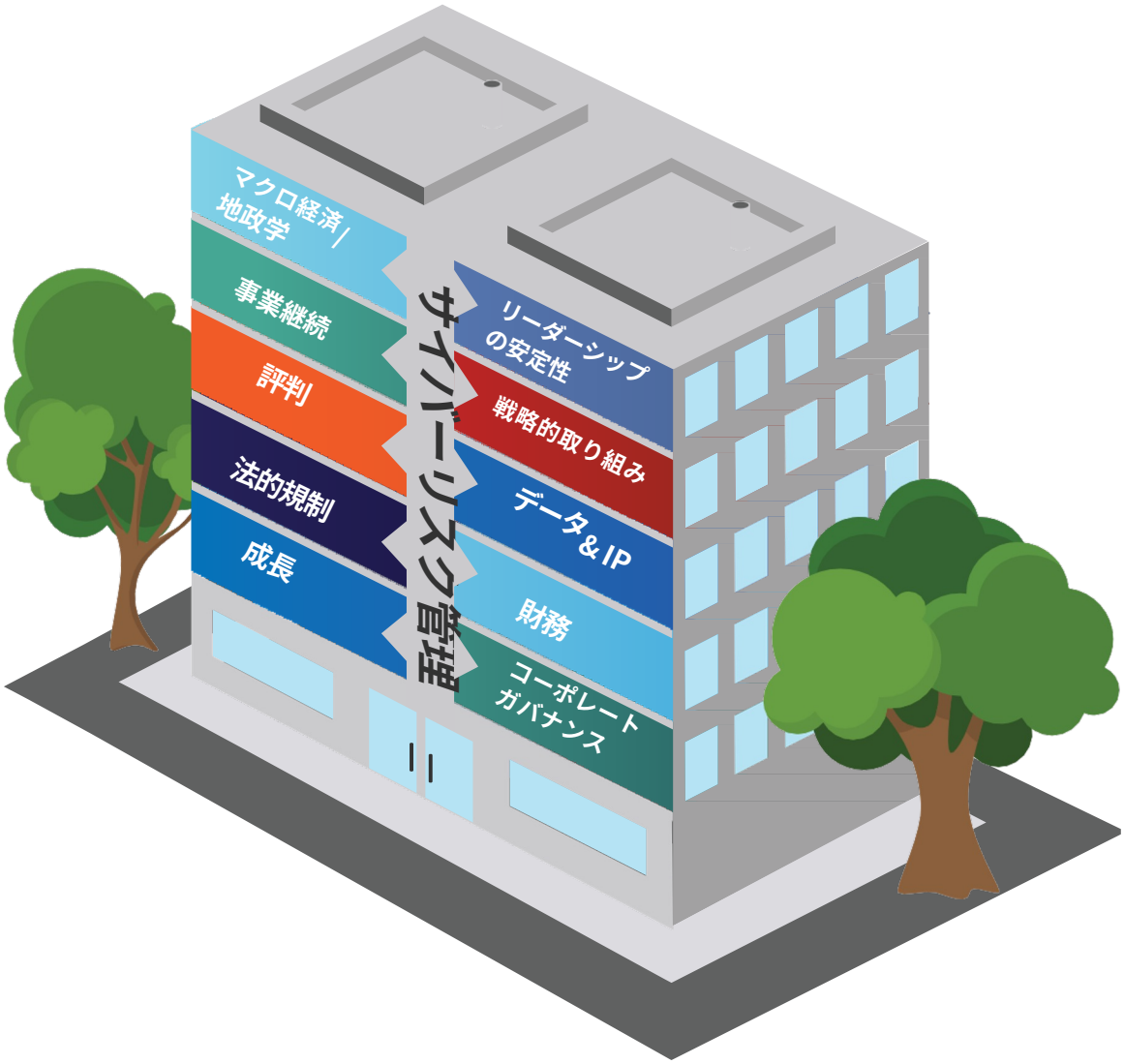


図03：適切なサイバーリスク管理は、取締役会が監督するあらゆる機能分野にまたがる。

どのようなサイバー戦略を採用するかに関わらず、取締役会のメンバーは、自組織のプロセスの成熟度を理解することが重要です。現在、多くの企業は、米国政府の国立標準技術研究所（NIST）[6]のフレームワークを基に、毎年または定期的に専門知識の評価を行っています。

6 National Institute of Standards and Technology (2023, August 17). NIST https://www.nist.gov/cybersecurity

通常、このような評価は、PWC、EY、Accentureなどの外部機関によって行われ、多くの場合、同業他社との比較も含まれます。先述の通り、SECは、経営陣と取締役会がサイバーリスクを評価・管理するためのプロセスについても定期的な開示を求めています。

追加ガイダンス

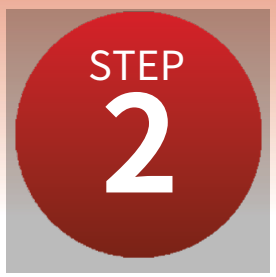
全米企業取締役協会（NACD）は、2023 Director's Handbook on Cyber-Risk Oversight（サイバーリスク監督に関する2023年取締役ハンドブック）と題する出版物の中で、取締役会のためのサイバーリスク管理の6つの原則を発表しました[7]。このハンドブックでは、以下の6つのテーマと指針が中心となっています：

1. 戦略的ビジネスイネーブラーとしてのサイバーセキュリティ
2. サイバーリスクの経済的要因と影響の理解
3. サイバーリスク管理とビジネスニーズの整合
4. サイバーセキュリティを確実にサポートする組織設計
5. サイバーセキュリティ専門知識の取締役会ガバナンスへの組み込み
6. 組織的な回復力と協力体制の促進

7 この出版物は、対象事項に関して正確な解説を提供することを目的としています。本書は、著者および発行者である全米会社役員協会およびインターネット・セキュリティ・アライアンスのいずれも、本書を通じて法律、会計、またはその他の専門的なサービスを提供するものではないことを理解した上で提供されています。法的助言または専門的支援が必要な場合は、資格を有する有能な専門家のサービスを求める必要があります。

キーポイント

- 取締役会はサイバーリスク管理において主要な役割を果たす。取締役会は、自組織が直面しているテクノロジー関連のリスクをより深く理解し、監督する必要がある。
- 取締役会は、自組織の技術的能力とプロセスについて基本的な理解を持つべきである。これは、サイバーセキュリティに関する投資の意思決定に役立つ。
- 取締役会は、支出の優先順位を設定する際に、組織がどの程度サイバーリスクへさらされているかを検証・評価すべきである。より広範なリスク対策計画の一環としてサイバーセキュリティに焦点を当てること。
- 責任の明確化、インシデント対応計画、準備演習などの予防的措置が重要である。組織内でのサイバーに対する意識を高めていくことも重要となる。
- 取締役会のメンバーにはサイバーセキュリティの専門家を配置すべきである。NIST や NACD のような組織は、効果的なサイバーリスク管理に関するガイダンスを提供している。



優先順位を上げる

ビジネスリスクの鍵となる要素としてのサイバーリスク

なぜこのステップが重要なのか？

サイバーリスクはビジネスリスクです。組織のブランドや評判を脅かし、数百万ドルから数十億ドルという大きな経済的影響や株主価値の損失を引き起こす可能性があります。軽微なものから深刻なものまで、さまざまな影響を引き起こすサイバー攻撃が存在し、備えのない組織はビジネスに大きな影響を受けやすくなっています。サイバー攻撃者は、懸命に組織の弱点を見つけようとしており、彼らの攻撃範囲、技術の洗練度、戦略は、多くの組織の防御能力よりも速く進化しています。攻撃者は、訓練を受けていない人材、外部に露出している資産、保護されていないデータ、脆弱な物理的セキュリティ、管理されていないエンドポイントデバイス（PCや携帯電話）など、企業を攻撃するあらゆる方法を模索します。

取締役会は何をすべきか？

サイバー攻撃についての全般的な知識を理解することは、サイバーリスクを優先順位付けする上で役立ちます。サイバー攻撃とは、攻撃者が組織の人員、インフラ（資産やテクノロジー）、および/またはデータへの不正アクセスを試みることです。攻撃者は、外部の者（犯罪者、競合他社、国家に支援された組織など）である場合もあれば、内部の者である場合もあります。内部の脅威者は、国家機関から送り込まれたもの、敵対的な従業員（悪意や恐喝などによるもの）、または不注意なユーザー（意図的でないもの）である可能性があります。脅威の勢力は進化し続け、かつてないスピードで活動を拡大しており、多くの脅威グループは潤沢な資金を有しています。国家的行為者（政府や政府関係者）

サイバー攻撃者の攻撃範囲、洗練度、戦略は、多くの組織の防御能力よりも急速に進化しています。

は、攻撃の洗練度と能力を高め、特定の組織を標的とした高度な攻撃を計画しています。適切なセキュリティ管理や重層的な防御策が不十分な組織や、脆弱なインフラを使用している組織は、悪意を持った行為者によって、より大きなサイバーリスクにさらされています。

サイバーリスクは、組織のシステムに優先的にアクセスできる顧客やサプライヤーなどの「信頼された」パートナー企業からも発生します。これは、組織が外部パートナーの持つ脆弱なテクノロジーを統合した場合に発生する、あまり目立たない形のサイバーリスクです。もし、統合されているが悪用されているリソースを検出する手段を備えていない場合、敵対者があなたの組織の環境内で自由に行動できてしまう可能性があります。

国家による支援を受けているサイバー攻撃は極めて巧妙であり、その実行者も非常に有能です。彼らは、組織の最も脆弱な箇所を見つけ、最も機密性の高い領域にアクセスし、データを抜き出す能力を繰り返し見せつけてきました。我々がこれまで目にしてきたような、単一の侵入経路から組織が大きく破壊される事例は、今後も発生することになるでしょう。

巧妙な攻撃者は、さまざまな悪意のある行為を行う可能性があります。

- 日常業務を中断させる
- コンピューターを使用不能にする
- 組織のデータへのアクセス権を剥奪し、拒否する
- 独自の洞察を得るためにシステム内の活動を管理する
- データを収集し盗む
- 情報または技術システムを破壊する
- 他のシステムに対する攻撃を開始するために侵害されたコンピュータを使用する

サイバー攻撃の基礎

サイバー攻撃は通常、無差別型攻撃と標的型攻撃の2つに分類されます。無差別攻撃では、攻撃者は、できるだけ多くの人間やテクノロジーを悪用することに焦点を当てます。一方、標的型攻撃では、攻撃者は特定の組織、部門（開発部門など）、または個人（CEOの秘書など）を狙います。

サイバー攻撃（侵害とも呼ばれる）には主に4つのタイプがあります。

- **フィッシング**：犯罪者がソーシャル・エンジニアリングを用いて、銀行やリーダーなど信頼できる情報源になりすまし、機密情報を渡すよう説得する。
- **ランサムウェア**：犯罪者が情報システムに悪意のあるソフトウェアを仕込んでデータをロックまたは暗号化し、身代金を支払うまでアクセスできないようにする。
- **マルウェア**：技術システムを攻撃し、データやクレジットカード情報を盗んだり、スパイウェアを仕 込んでシステムの活動を管理したりするなど、能動的に損害を与えるために開発された悪質なソフトウェア。
- **内部脅威**：機密データにアクセスできる組織内部の人間が、時には無意識のうちに引き起こすデータ侵害。

サイバー攻撃は組織のビジネスに非常に大きな被害を与えます。

- **顧客／ユーザー情報の窃盗**：犯罪者は、多くの場合、音声、電子メールアドレス、Slack、その他の通信手段を使ったなりすましによって、機密性の高い個人情報を狙う。
- **知的財産、企業秘密、非公開情報の窃盗**：犯罪者は組織の最も重要なデータを狙う。
- **サービス妨害**：犯罪者は、公共のウェブサイト、電子メール、ノートパソコンなどのサービスへのアクセスを積極的に妨害する。

ランサムウェアに要注意

Zscaler 2023 Ransomware Reportによると、全世界でのランサムウェア攻撃は前年比で40%近く増加しています。また、同レポートでは、以下のことが明らかになりました。

- ランサムウェアの影響は特に米国で深刻であり、過去12ヶ月間のランサムウェア・キャンペーンの約半数が米国を標的としていた。
- 芸術、娯楽、レクリエーション業界の組織へのランサムウェア攻撃が最も急激に増加し、増加率は430%を超えた。
- 製造業は依然として最も標的とされる業種であり、ランサムウェア攻撃全体の15%近くを占める。次にサービス業が続き、昨年のランサムウェア攻撃総数の約12%を占めている。

「ゼロデイ」攻撃とは、これまでに発見されていない脆弱性を悪用してハードウェアやソフトウェアを攻撃する手法です。このような攻撃は、一般的に、民間組織、政府機関、重要なインフラ機関で数百万人が使用している技術を標的とします。ゼロデイ攻撃は、マクロ経済的な損害、公衆衛生への影響、国家安全保障に脅威をもたらす可能性があります。実際、最近の報告書[8]によれば、一般的なファイアウォールの70%にゼロデイ攻撃に対する脆弱性があり、これは攻撃者が悪用可能なインスタンス30万件以上に相当します。組織に対し真のゼロデイ攻撃が発生した場合、事後対応やコミュニケーション活動において、取締役会メンバーの集中的な関与が必要となる可能性があります。

8 (n.d.). 2023 ThreatLabz State of Ransomware. Zscaler. https://info.zscaler.com/resources-industry-reports-2023- threatlabz-ransomware-report

最近のサイバーセキュリティ侵害の急増により、数十億ドルの損害が発生している

図04：2019年後半以降に発生した主なサイバー侵害25件の概要

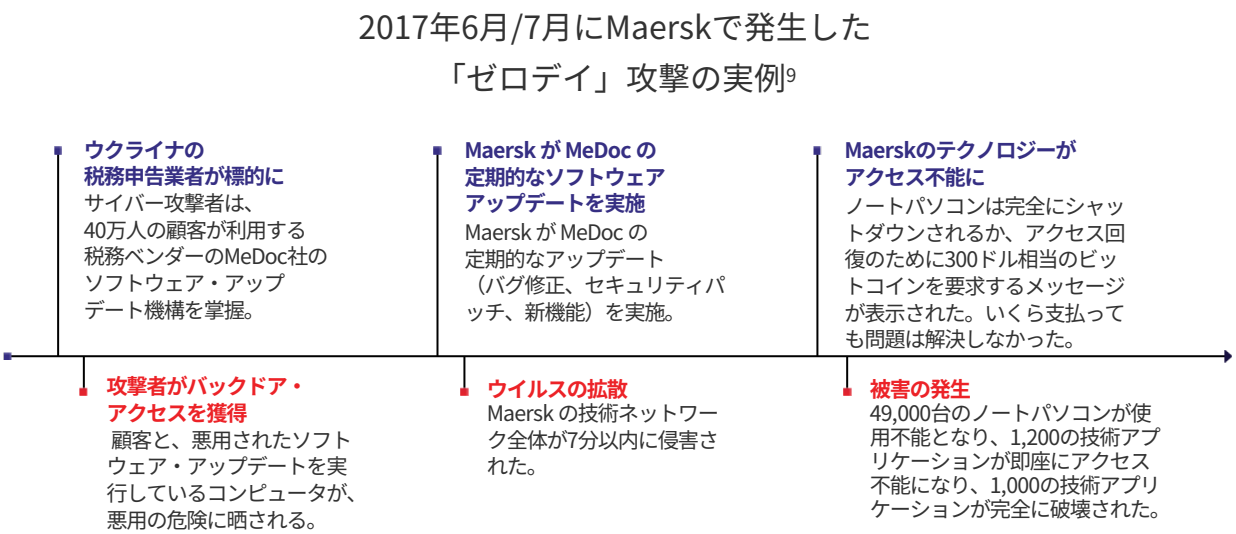


図05：Maersk社におけるデータ侵害の詳細。

2021年に発生したColonial Pipelineへの攻撃の概要

Colonial Pipeline[10]は米国最大の石油精製品パイプラインで、消費者のエネルギー需要を満たすために毎日1億ガロン以上の燃料を輸送しています。2021年5月、同社はサイバー攻撃を受け、米国の一般市民や企業に全国的な影響を及ぼす事態となりました。

攻撃者はまず、Colonial Pipelineのユーザーのログイン認証情報を盗みました。サイバーセキュリティと技術ソリューションが脆弱な状態にあったため、攻撃者はすべてのシステムとデータにアクセスすることができました。攻撃者は価値の高い請求アプリケーションを標的にし、データを身代金要求のために保持し、その結果、Colonial Pipelineは440万米ドルの身代金を支払うことになりました（ただし、230万米ドルは後に米国連邦法執行機関によって回収）。

9 WIRED (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired.com. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
10 (2022, April 26). Colonial Pipeline hack explained: Everything you need to know. TechTarget. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

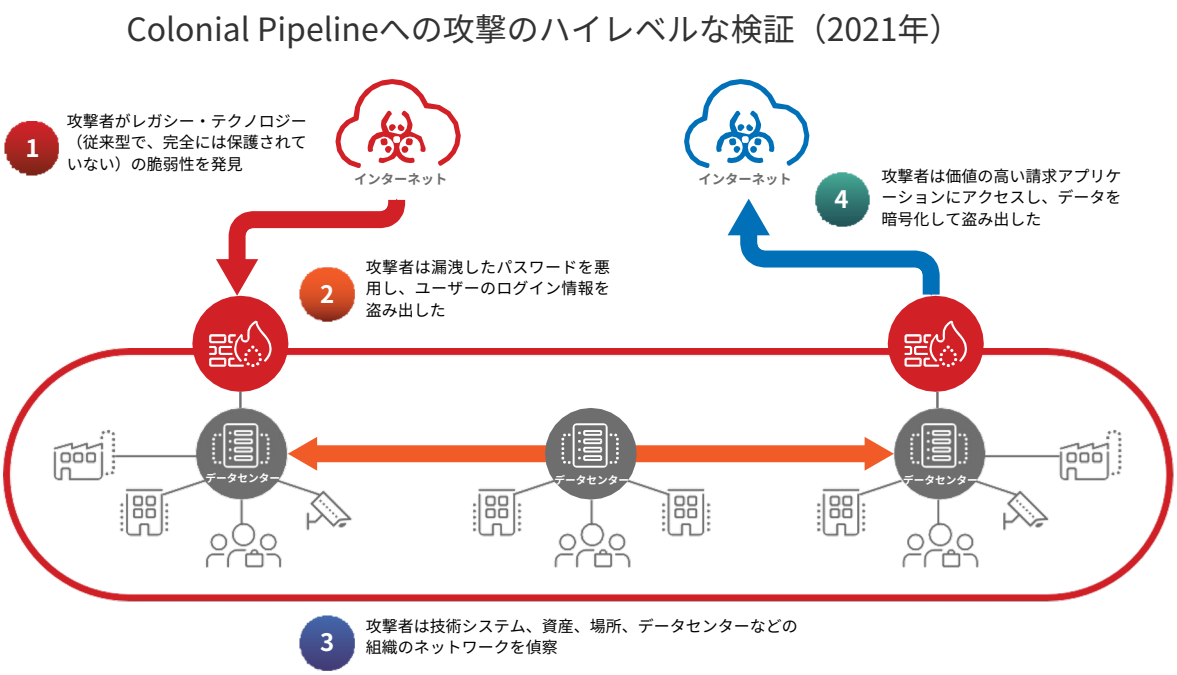


図06：Colonial Pipelineへのデータ侵害の詳細。

この攻撃によって、様々な影響が引き起こされました。

- 身代金として440万米ドルの支払い
- 2時間以内に～100GBの機密データが盗まれた
- パイプラインと業務の6日間の停止
- 風評への甚大なダメージ
- 連邦政府の関与と議会公聴会

この侵害は重要なインフラに被害を与えため、社会により大きな影響をもたらしました。NISTは、重要インフラを「物理的であるか仮想的であるかを問わず、米国にとって極めて重要なシステムおよび資産であり、もしそれらに機能不全や破壊が生じた場合、安全保障、国家経済安全保障、国民の健康もしくは安全、またはそれらの組み合わせに深刻な影響を及ぼすもの」と定義しています。

攻撃による影響は様々なところに波及しました。

- 数万人がガスを利用できず、17以上の州が非常事態を宣言
- 数百万人のガス料金が高騰
- パイプライン事業者の45%に影響
- 航空会社および航空物資輸送便に影響
- 経済的な影響が波及

こうしたリスクを考慮すると、組織が競争力を維持し生き残るためには、継続的な技術的進化（すなわちデジタルトランスフォーメーション）を遂げなければなりません。競争力を維持するためには新たなテクノロジーを採用する必要があり、これには、パートナー企業やサードパーティとの安全なデータ共有も含まれます。また、アプリケーションやインターネット、クラウドへのアクセスを地理的な制約なく安全に提供する方法を見つける必要があります。企業は、保護された状態を維持するために、成長、革新、買収を止めることはできないのです。

このような変革が起こる中、現在使用されている従来型のサイバーセキュリティ・ソリューションの多くは、不正アクセスを防止するには十分ではありません。それにも関わらず、多くの組織が多くのIT予算をサイバーセキュリティに費やしています。それでも侵入されてしまうのはなぜでしょうか？それは、多くの場合、古いテクノロジーにお金を費やし、セキュリティの欠陥を応急処置的に修正し、全体的なサイバーリスクの解決には効果のない新しいテクノロジーを衝動的に採用しているからです。このようなアプローチは、既存の時代遅れの技術を複雑にし、運用上の摩擦とコストを増大させます。

こうしたリスクを考慮すると、組織が競争力を維持し生き残るためには、継続的な技術的進化（すなわちデジタルトランスフォーメーション）を遂げなければなりません。

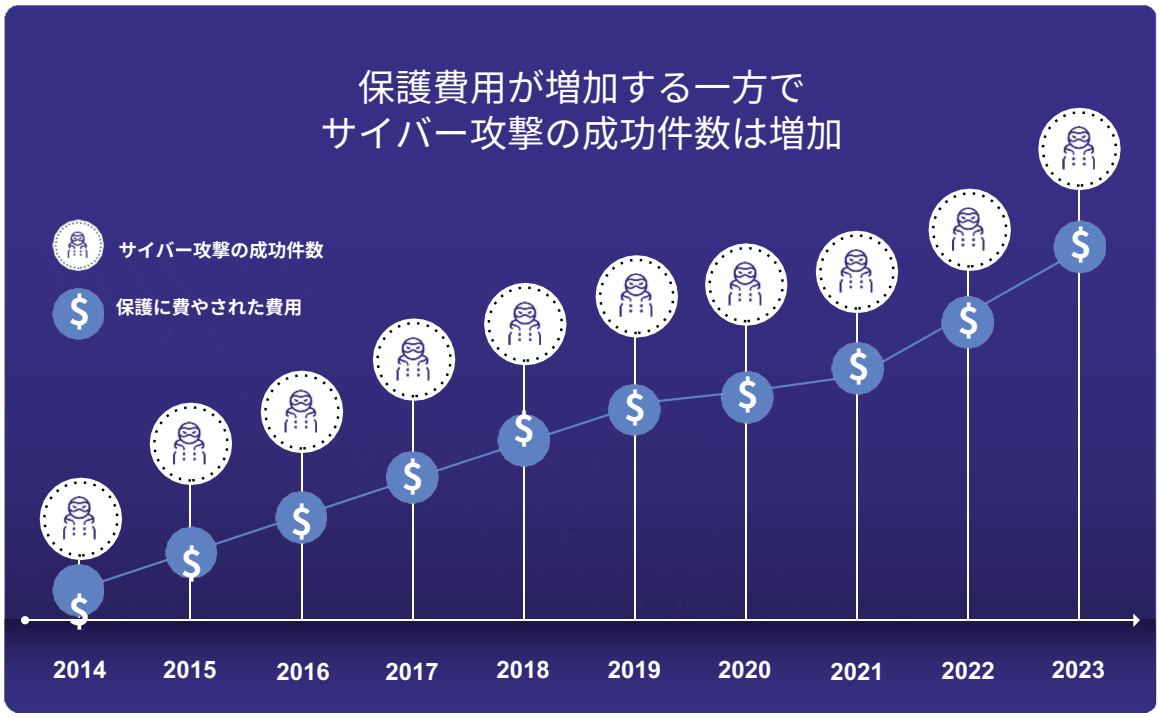


図07：保護費用が増加しても、サイバー攻撃の成功件数は増加。

組織がネットワークとサイバーセキュリティに多額の費用を費やしたにもかかわらず、なぜ侵入されてしまうのか、もう少し掘り下げてみましょう。主な問題は、80年代後半から90年代前半に設計され、そして現在も使用されているサイバーセキュリティ技術が、「暗黙の信頼」型のアーキテクチャーを中心にしていることです。これは、各企業のネットワークがほとんど相互に接続されていなかった時代には問題なく機能していました。主要なネットワーク・ハードウェアおよびソフトウェア企業は、企業がデータへの組織的アクセスをすべてのユーザー、支店、倉庫、工場、サプライヤーなどに拡張できるように、優れた技術を開発しました。

しかし、クラウドとモビリティの台頭により、ビジネスのやり方は大きく変わりました。データは今やあらゆるところに存在しており、従業員はどこからでもリソースにアクセスできる必要があります。組織は、クラウド時代に旧世代のネットワーキングとセキュリティの慣行を持ち込みましたが、その技術には拡張性がないことに気づきました。

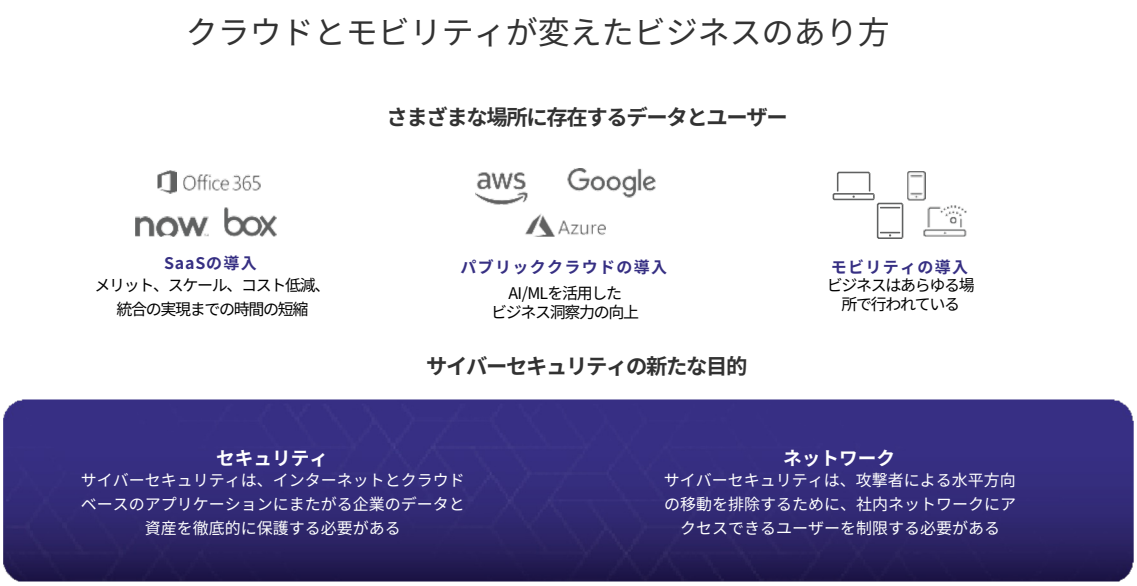


図08：SaaS、パブリッククラウド、モビリティは、ネットワークとセキュリティの目的を変えた。

このサイバーセキュリティ・モデルでは、従業員が信頼されたネットワークへのアクセスを許可されると、その従業員（または攻撃者）は水平方向の移動が可能になり、会社の管理下にあるすべてのオフィス、工場、デバイスにアクセスできます。アプリケーションも同じ社内ネットワーク上にあり、組織の重要なリソースはすべて横断可能な（ネットワーク用語で言うとルーティング可能な）1つの空間に置かれています。このような従来型のネットワークは、当時においては連携と分散コンピューティングにおける大きな進歩でしたが、今日では、このようなアーキテクチャーは、午前3時に玄関のドアを開けておき、家の中を見知らぬ人に自由に歩き回らせているのと同じようなものです。

つまるところ、この従来のアプローチでは、現代の世界に適応することができないのです。しかし、多くの組織はいまだにこの種のテクノロジーを使用しており、そのため頻繁にサイバー攻撃の標的となっています。今日では、労働者のモバイル化がかなり進み、自宅で仕事をする人も増えています。組織は、仮想プライベート・ネットワーク（VPN）を使って会社のネットワークを各従業員の所在地に拡張することで対応しようとしてきました。確かにVPNは一定レベル

の保護を提供しますが、その一方で、一般に公開されており、ネットワークレベルでの接続が行われるため、多くの侵害の原因ともなっています。結局のところ、VPNは、悪意ある行為者が会社のネットワークにアクセスする新たな機会を作り出しているのです。

この状況で、パブリッククラウドやSaaSを導入するとどうなるでしょうか。従来のアーキテクチャーでは、ユーザーとアプリケーションを同じネットワーク上に置いていたため、企業ネットワークが、クラウドのさまざまな場所すべてに拡張されることになります。従来のネットワークモデルが拡大するにつれて、ユーザーだけでなく攻撃者にとっても水平移動を可能にする巨大な攻撃対象領域が形成されることになります。

一般にハブ・アンド・スポーク型ネットワークや「城と堀」型セキュリティとして知られるこれらの古いアーキテクチャーは、今日でも多くの組織で採用されています。

図09：従来型のアーキテクチャーは城と堀のようなもので、モバイルとクラウドの世界ではセキュリティを提供できない。

企業での窃盗を例にとると、企業がネットワークやセキュリティに何百万ドルも費やした後でも、攻撃者が組織に侵入するためにとる4つの重要なステップが存在します。

図10：典型的なサイバー侵害の4つの段階。

1 オフィスを発見する (外部に面した攻撃対象領域)

悪人は、あなたの公開されている攻撃対象領域を見つけます。攻撃対象領域とは何でしょうか？インターネット上で発見可能な、暗黙のうちに信頼されているネットワークアドレスはすべて攻撃対象となります。人々やテクノロジーの間でデータが移動する際に適切に暗号化されていないなど、脆弱性を持つシステムはすべて侵害される可能性があります。到達が可能であれば、侵入も可能ということです。

2 脆弱な入口を使って侵入する (不正アクセス)

悪人はあなたのネットワークに侵入しました。外部からの侵入はすべてインターネットから行われ、無防備なユーザーや保護されていないデバイスなど、侵害するための弱点を探します。いったん資産が侵害されると、攻撃者はその侵害されたリソースを起点として、さらなる攻撃を行います。

3 企業の機密情報を探す(水平方向の移動)

悪人はネットワークに侵入し、水平方向に移動して価値の高いターゲットを探します。VPNは企業ネットワーク上にあるため、ハッカーはVPNを使って企業内を横断し、あらゆるシステムやアプリケーションをダウンさせることが可能です。あるいは、データを暗号化して身代金を要求することもできます。これを脆弱性毎に修正していくのは、高速道路に料金所や有料道路を作ってアクセスを規制するようなものです。

4 機密情報を持って立ち去る (データ流出)

悪人はあなたのデータを盗みました。盗まれたデータは、通常インターネットを介して送信されます。データは組織の重要な財産であり、その盗難は知的財産の損失、顧客からの信頼の失墜、ブランド力への悪影響を意味します。

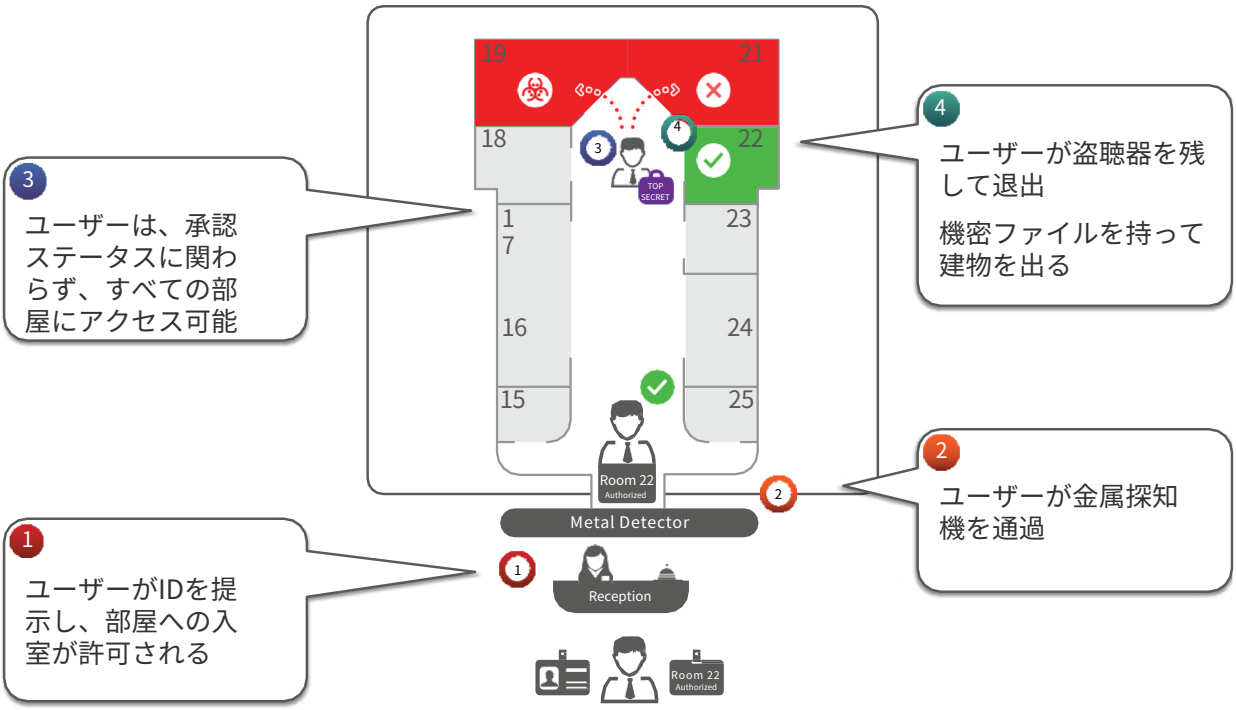


図11：従来のセキュリティは、受付でチェックインした後、付き添いのない訪問者がオフィスビル全体を自由に歩き回れるようにしているようなものだ。

キーポイント

- サイバー攻撃は、財務、風評、業務に大きな影響を与える脅威である。予防策のない組織は深刻な影響を受けやすくなっている。
- 攻撃者は脆弱性を悪用し、システム、データ、インフラに不正アクセスを試みる。攻撃が成功すると、データが盗まれ、ビジネスが大きな混乱に陥る可能性がある。
- 暗黙の信頼に基づく従来のネットワーク アーキテクチャーは、データとアクセスがあらゆるところに存在する今日では十分ではない。しかし、多くの組織がいまだにこのような時代遅れのモデルに依存している。
- 攻撃者は、攻撃対象領域を見つけ、システムに侵入し、水平方向に移動し、データを盗むという手順を踏む。多額の費用を費やしている組織であっても、侵入される可能性がある。
- Colonial Pipelineへの攻撃は、たったひとつの漏洩した認証情報がすべてのシステムへのアクセスを可能にし、全国的な燃料不足と金銭的被害、風評被害を引き起こしたことを示している。

評価

組織の現在のサイバー脅威対策と成熟度レベル

なぜこのステップが重要なのか？

問題が影響を及ぼす範囲を理解しなければ、その問題に対処することはできません。組織がどの程度侵害されやすいかを判定することは、一般にサイバーリスク管理体制の評価と呼ばれます。サイバーリスク管理体制とは、組織がサイバーに関する脅威やリスクから自らを守る能力のことです。取締役会がサイバーセキュリティのために多額の予算を承認したとしても、リスクが最小であるとは限りません。

取締役会は何をすべきか？

組織のサイバーリスク管理体制を確認するには、CIO、CISO、またはCROに以下の質問をする必要があります:

1. 我々の組織にはどのようなサイバー攻撃対象領域があるか？よりリスクの高い古いネットワーク・アーキテクチャーやセキュリティ・アーキテクチャーをいまだに利用しているか？つまり、外部から到達・侵入が可能か？これらの質問には、製造装置や医療機器などの運用技術（OT）やモノのインターネット（IoT）のような物理的資産も含まれることを明確にしておく。
2. 誰が我々を攻撃しようとしているのか？これには、外部攻撃者と内部攻撃者の両方を含む。
3. 攻撃を防止または軽減するために、どのようなポリシー、手順、または管理が導入されているか？
4. 組織が侵害された場合、どのような対応が計画されているか？例えば、内部のタイガーチーム（特命班）は、内部データや顧客データの漏洩に対処できる体制を整えているか？
5. 侵害された場合、攻撃者はネットワークを自由に移動して機密データを探し回ることができるか？現在のセキュリティ管理は、この移動を防ぐためにどの程度効果があるか？
6. 我々の機密データはどこに保管されているのか、また、攻撃者はそれを見つけることが可能か？この質問には、どのデータが最も価値があり、どこに保管されており、誰がアクセスでき、どのように使用されているのかを特定することも含まれる。

7. 攻撃者は我々の機密データを盗むことができるか？データが盗まれた場合、それが組織の評判、財務の安定性、製品やサービスを提供する能力にどのような影響を与えるか？
8. 重要なデータや資産にアクセスできる社内の従業員やサードパーティの管理をどの程度行なっているか？これらの人物がデータや資金を組織外に持ち出すことは可能か？
9. 侵害が発生した場合、被害の程度を評価し、修復を支援するための外部リソースとの契約を締結しているか？

サイバーリスク管理体制とは、サイバー上の脅威やリスクから自らを守る組織の能力を指します。たとえ理事会がサイバーセキュリティのために数百万ドルを承認したからといって、リスクが最小になるわけではありません。

これらの質問に答えることは、サイバーリスク管理体制を評価する上で最も重要なステップです。第三者による監査は、組織の現状を独立した視点からと評価するのに役立ちます。これらの監査では、以下の4つの観点からリスクを評価することに重点を置いています：

- **外部に面した攻撃領域** – 今現在インターネット上で公開されている、攻撃者によるデータや技術の悪用を可能にする脆弱性を調査する。
- **データ侵害** - 悪意のあるコンテンツが組織内に入り込んだり、組織内で共有されたりする可能性を評価する。
- **水平方向の移動** -攻撃者が侵入に成功した後に発見できる、同じネットワーク上にあるアプリケーションとデータがどの程度存在するかを測定する。
- **データ損失** -どのような機密性の高い組織データが窃取され、悪用されるリスクがあるかを理解し、内部データ共有プラクティスの安全性を評価する。

これら4つのリスク要素をモニタリングし、ダッシュボード形式（下図を参照）で提供することで、現状と時系列での傾向を完全に透明化することができます。

図12：サードパーティのリスク評価の例（出典：Zscaler）

評価終了後、取締役会のメンバーは目標を設定し、組織の進捗状況を時系列で把握する必要があります。これら4つの分野のスコアに大きなマイナスの変化が起きた場合には、経営陣とともに最優先で取り組むべきです。

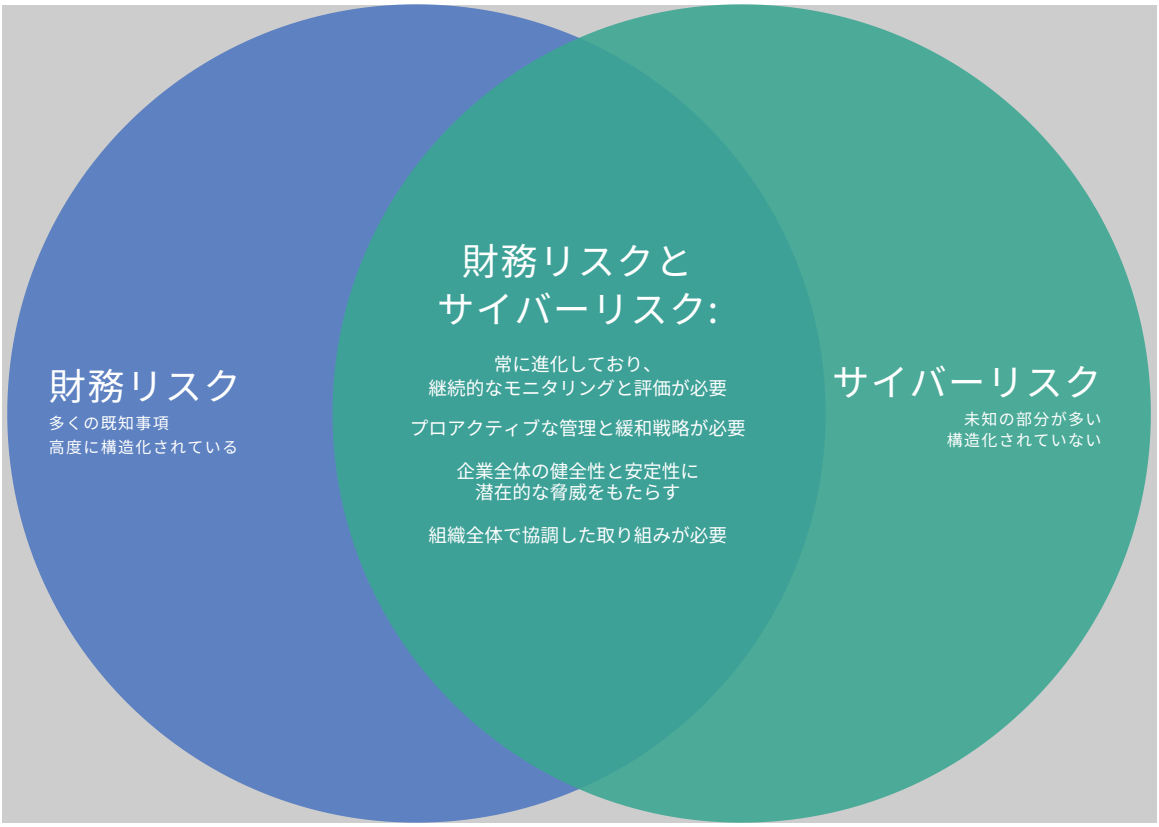


図13：サイバーリスクと財務リスクには、その対処方法においていくつかの共通点がある。

おそらく、あなたは受託者責任の一環として、財務リスクの評価にすでに高い意識をお持ちでしょう。財務リスクとサイバーリスクには類似点と相違点があります。財務リスクは構造化されており、多くの既知の要素が存在しますが、サイバーリスクは反対に、多くの未知の要素が存在し、構造化されていません。

悪質な行為は、予期せぬ金銭的損失や業務の中断など、ビジネスに大きな影響を与える可能性があり、最悪の場合、企業は倒産に追い込まれることもあります。

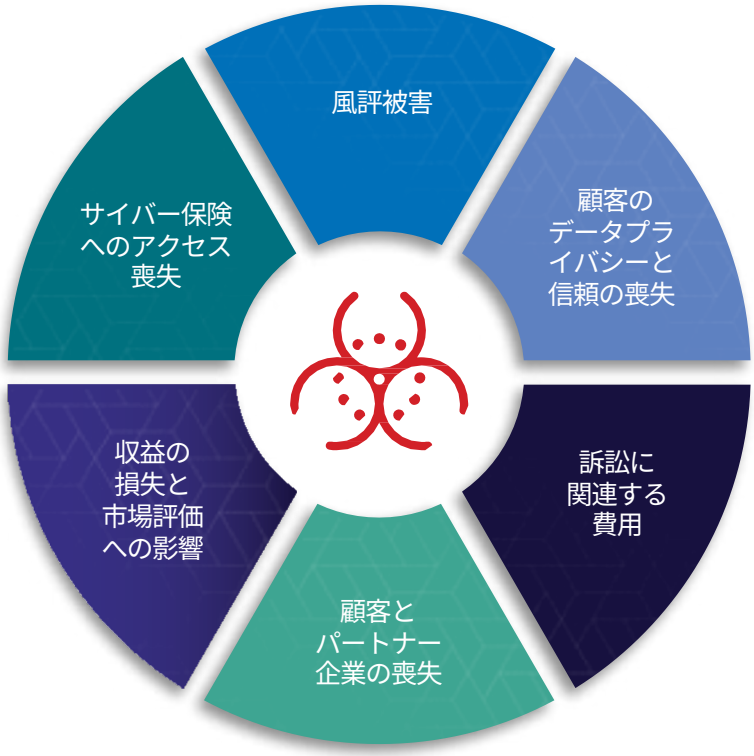


図14：サイバー攻撃のビジネスへの影響。

サイバー攻撃は企業の財務的安定性を脅かすため、全従業員と利害関係者にとって共通の関心事であり、責任でもあります。以下の情報は、サイバー侵害の損失見積りを策定するための大まかな出発点となります：

- データ漏洩の平均コスト：435万ドル[11]
- 流出した記録1件あたりの平均コスト：164ドル[12]
- サイバー攻撃から回復するまでの平均日数: 279日[13]
- 重大なプライバシー侵害に対する罰金：
  企業の年間グローバル収益の最大4%[14]

11 International Business Machines (n.d.). Cost of a Data Breach Action Guide. IBM. Retrieved August 17, 2023, from https://www.ibm.com/reports/data-breach-action-guide
12 (n.d.). Worried About a Cyberattack? What It Could Cost Your Small Business. Business News Daily. Retrieved August 17, 2023, from https://www.businessnewsdaily.com/8475-cost-of-cyberattack.html
13 (2022, September 22). Cyberattack recovery time and cost much higher than businesses realize. Nationwide. https://news.nationwide.com/cyberattack-recovery-time-and-cost-much-higher-than-businesses-realize/
14 (2022, January 18). Fines for breaches of EU privacy law spike sevenfold to $1.2 billion, as Big Tech bears the brunt. CNBC. https://www.cnbc.com/2022/01/18/fines-for-breaches-of-eu-gdpr-privacy-law-spike-sevenfold.html

図15：サイバー侵害による推定損失額。

機密データ流出に対する罰則

- 欧州連合の一般データ保護規則（GDPR）：重度の違反の場合、最高2,000万ユーロまたは当該企業の全世界での収益の4%のいずれか高い方。
- 米国医療保険の相互運用性と説明責任に関する法律（HIPAA）：違反1件につき50～50,000米ドル、最高罰金は150万米ドル。
- カリフォルニア州プライバシー権法（CPRA）：違反1件につき最高2,500米ドル、または故意1件につき最高7,500米ドル。故意による違反の場合は1回につき7,500米ドル。罰金の上限なし。

サイバーリスクを理解することに加え、組織がサイバーインシデントにどのように対応するかを決定することも重要です。サイバー脅威の予防、検出、対応に関する戦略を盛り込んだサイバーリスク管理計画は用意していますか？サイバーセキュリティ成熟度モデルを使用して、現在の状態を「未準備」、「事後対応型」、「事前対応型」、「予測型」と評価することができます。ほとんどの組織は、自社を「未準備」または「事後対応型」と評価するでしょう。なお、NISTでは、サイバーリスクのスコアリングに関するフレームワークも提供しています。

15 National Institute of Standards and Technology (2021, February 1). NIST Cyber Risk Scoring. NIST. https://csrc.nist.gov/ CSRC/media/Presentations/nist-cyber-risk-scoring-crs-program-overview/images-media/NIST%20Cyber%20 Risk%20Scoring%20(CRS)%20-%20Program%20Overview.pdf

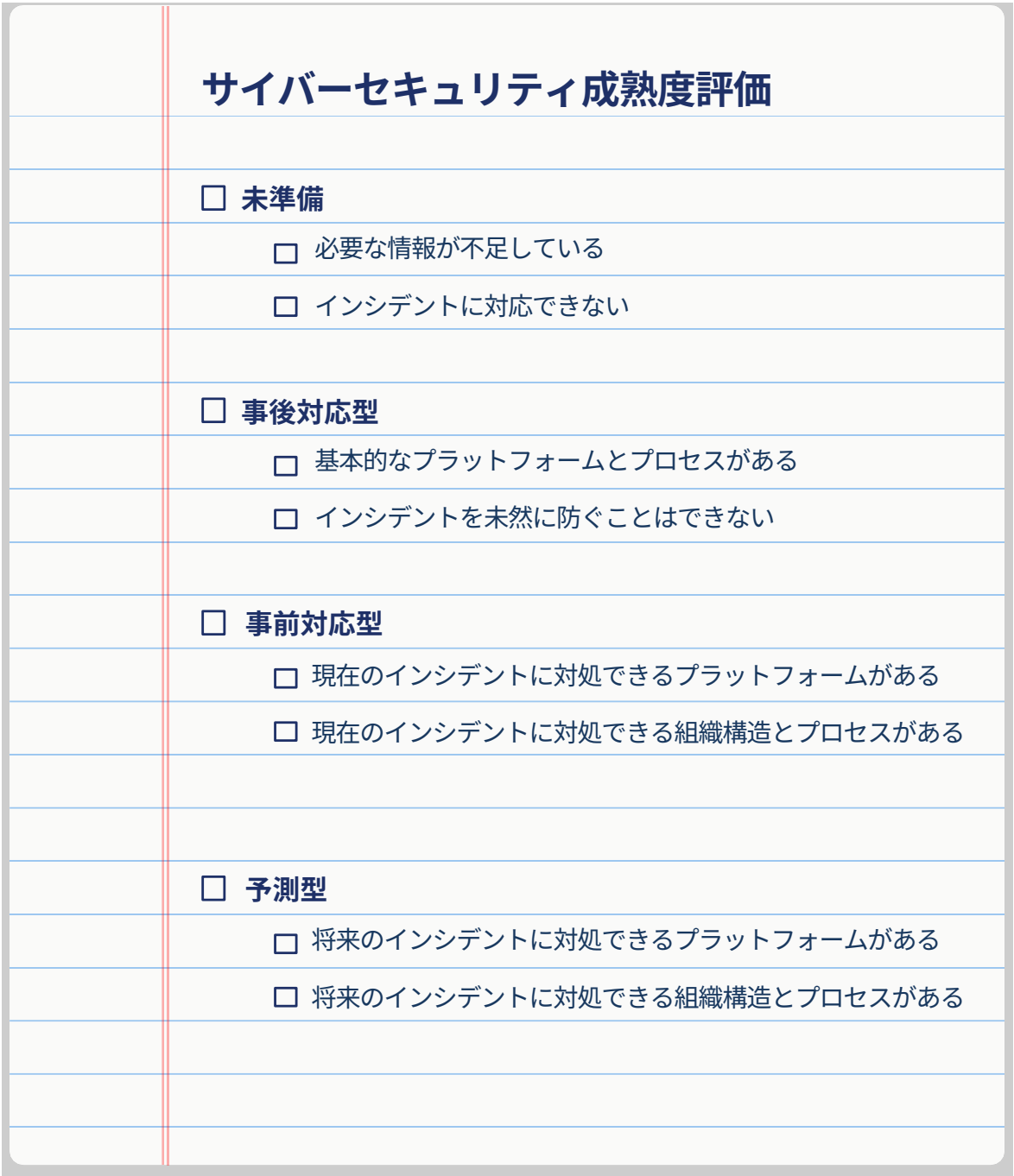
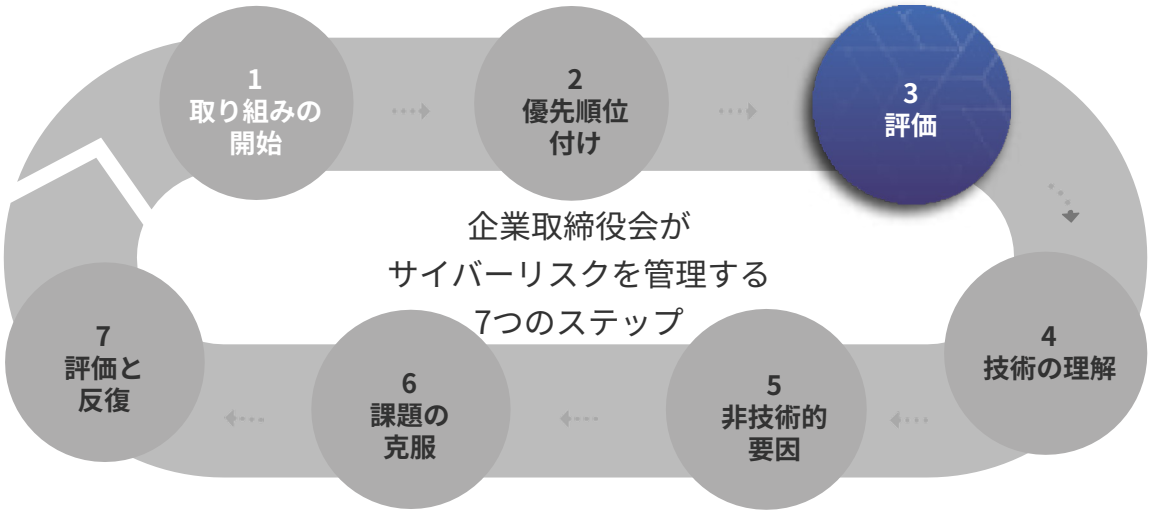
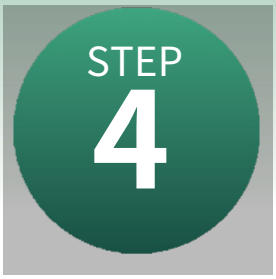


図16：サイバーセキュリティの成熟度は、準備ができていないものから予測可能なものまで幅広い。

キーポイント



- 公開されている攻撃対象領域、潜在的な攻撃者、既存のポリシーと管理方法、攻撃者のシステム内移動の可否、 機密データの場所とアクセス性、モニタリングの実施状況について質問することで、サイバーリスク管理体制を把握する。
- 第三者による外部攻撃対象領域、内部侵害、水平移動、データ損失の監査によって、独立した視点からリスクを評価することができる。
- サイバーリスクの評価では、不正侵入と罰金による損失を出発点として、財務的影響の分析を行う。
- 未準備、事後対応型、事前対応型、予測型のようなモデルを使用して、サイバーインシデント対応の成熟度を判断する。ほとんどの組織は未準備か、事後対応型の状態にある。
- サイバーリスクは、企業の安定性を脅かすものであり、全従業員および利害関係者にとって共通の関心事である。取締役会は、サイバーリスクの状況と傾向について、完全かつ最新の透明性を提供されるべきである。



技術の理解

ゼロトラスト・アーキテクチャーがビジネスリスクをいかに軽減するか

なぜこのステップが重要なのか？

組織のサイバーリスク管理体制が決まれば、サイバーリスクを軽減するために必要なテクノロジーの採用について議論することができます。多くの場合、適切な技術とアーキテクチャーの選択、調達、採用を実行するには、取締役会の十分な精査が必要です。サイバーリスクを理解し、ゼロトラスト・アーキテクチャー（本章の主題である）やリスク軽減のためのテクノロジーといった実行可能な解決策について、情報に基づいた意見を述べることが非常に重要となります。

取締役会は何をすべきか？

組織のサイバーリスク管理体制を決定したら、今度はその改善に取り組む番です。新しい技術の選択、導入、保守の実行は技術担当役員やその配下の役割ですが、これらの決定に対する取締役会の理解と精査が重要です。

サイバーリスクを最小化するための第一歩は、何を守るべきかを見極めることです。格言にあるように、「すべてを守ろうとすれば、何も守れない」。

サイバーリスクを最小化するための第一歩は、何を守るべきかを見極めることです。「すべてを守ろうとすれば、何も守れない」という格言がありますが、これはサイバーセキュリティにおいても同様です。組織が最も重要なもの（クラウンジュエル）を見極め、ミッション・クリティカル（業務の遂行に必要不可欠）なリソースを優先的に保護することが重要です。多くの場合、組織は全体をカバーしつつ漏れのないセキュリティ計画を細部まで定義しようとするあまり、泥沼にはまってしまいます。これは長期的には重要なことですが、いくつかの簡単なステップを踏むことで、重要な資産のリスク管理体制を大幅に改善することができます。

一般的に、最も重要な資産『クラウンジュエル（王冠の宝石）』とは、企業の知的財産、顧客データ、財務アプリケーション、IoT/OTシステム（工場設備など）や、ビジネスを推進するための重要なアプリケーションを指します。棄損した場合にビジネスに大きな影響を与えうるものは、すべてこのリストに含まれます。

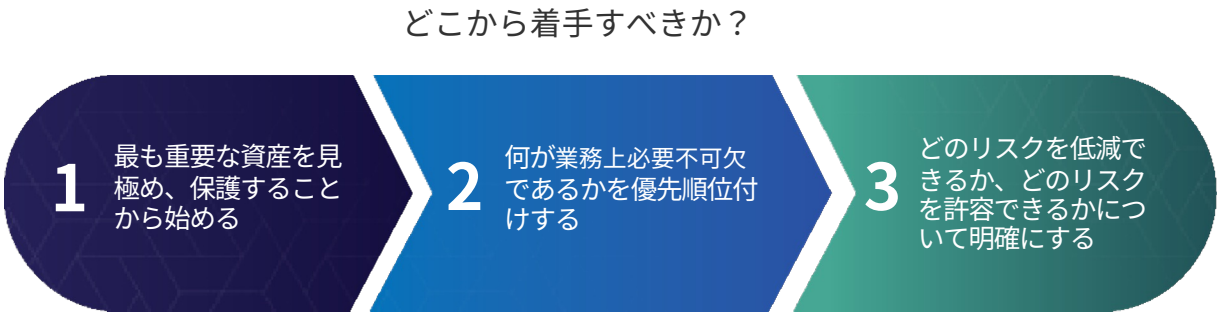


図17：保護すべきものを特定し、優先順位を付け、リスク対策を明確化する。

優先すべき資産が決まったら、組織にとって最大のセキュリティリスクの1つから対応します。それは、攻撃対象領域が存在し、侵入を許し、水平移動を許し、データ流出を引き起こす可能性があるにもかかわらず、暗黙のうちに信頼してしまっているアーキテクチャーです。このようなアーキテクチャーでは、ユーザー、アプリケーション、データは同じネットワーク上に置かれているため、その環境を侵害しようとする攻撃者により特定され、悪用される危険に晒されています。このような暗黙のうちに信頼しているアーキテクチャー（暗黙の信頼モデル）から脱却するには、ゼロトラスト・アーキテクチャー（ZTA）を採用する必要があります。

では、ゼロトラスト・アーキテクチャーとは何でしょうか？簡単に言えば、「決して信用せず、常に検証する」というアプローチをとることで、従来型アーキテクチャーの暗黙の信頼モデルを否定する（アーキテクチャーとテクノロジーによって実現される）理念です。ZTAは、ユーザーの身元確認に加え、ユーザーがどのような情報にアクセスしようとしているのかも考慮し、最小特権の原則（ユーザーが必要な最小限のアクセスのみを付与する）に基づいてアクセスを許可します。ZTAを導入することで、攻撃対象領域や水平移動を最小限に抑え、データの損失や漏洩の可能性を低減することができます。

ゼロトラスト・アーキテクチャーを理解するには、アプリケーション（および、その中に保存されたデータ）を2つに分類して考えてみましょう。

図18：ゼロトラスト・アーキテクチャーの特徴。

- プライベートアプリケーションは、IT部門によって組織内で管理されます。これらは多くの場合、企業のデータセンターでホストされるか、Microsoft、Amazon、Googleなどが提供するパブリッククラウドでホストされます。プライベートアプリケーションの中には、多くの機密データが保存されています。
- パブリックアプリケーションはサードパーティによって管理されます。これらは、Microsoft、Salesforce、ServiceNow、Workdayなどの企業が提供するSaaSソフトウェアアプリケーションです。公開されたインターネット上で使用されることが多いこれらのアプリケーションも、企業の機密データにアクセスすることができます。

これらのアプリケーションタイプはどちらも、業務上必要不可欠かつ機密のデータを保存しているため、ユーザー／デバイス、モノ（IoT/OT）、クラウド上のワークロードがそれらにアクセスする必要があります。しかし、ゼロトラスト環境では、基本的にこれらはすべて信頼されていません。ゼロトラスト・アーキテクチャーと従来のアーキテクチャーの最大の違いは、ZTAではユーザーとアプリケーションの間を直接繋ぐ、信頼されたネットワークが存在していないことです。では、どのように接続されるのでしょうか？安全な通信を実現するゼロトラスト・クラウドを経由して接続されます。ゼロトラスト・クラウドは、様々な登場人物（ユーザー、デバイス、アプリケーション）がどのようなネットワーク上からでも安全に通信できるよう、通信の交換所の役割を果たします。それにより、ユーザーはアクセスを許可されていないデータを見ることはできず、組織内の他の登場人物に接続することもできません。また、不適切なリソースへのアクセス試行の監視・管理が行われます。

ZTAは、ユーザーをアプリケーションやデータに接続する際の安全を確保し、リスクを軽減するためにいくつかの手順を踏みます。まず、すべての接続リクエストに対して、そのユーザーが誰なのか、何を求めているのか、どこへ行こうとしているのかを確認するためのチェックを行います。これはIDおよびアクセス管理の一部であり、認証情報が盗まれないようにするためには多要素認証（MFA）のような技術が重要です。

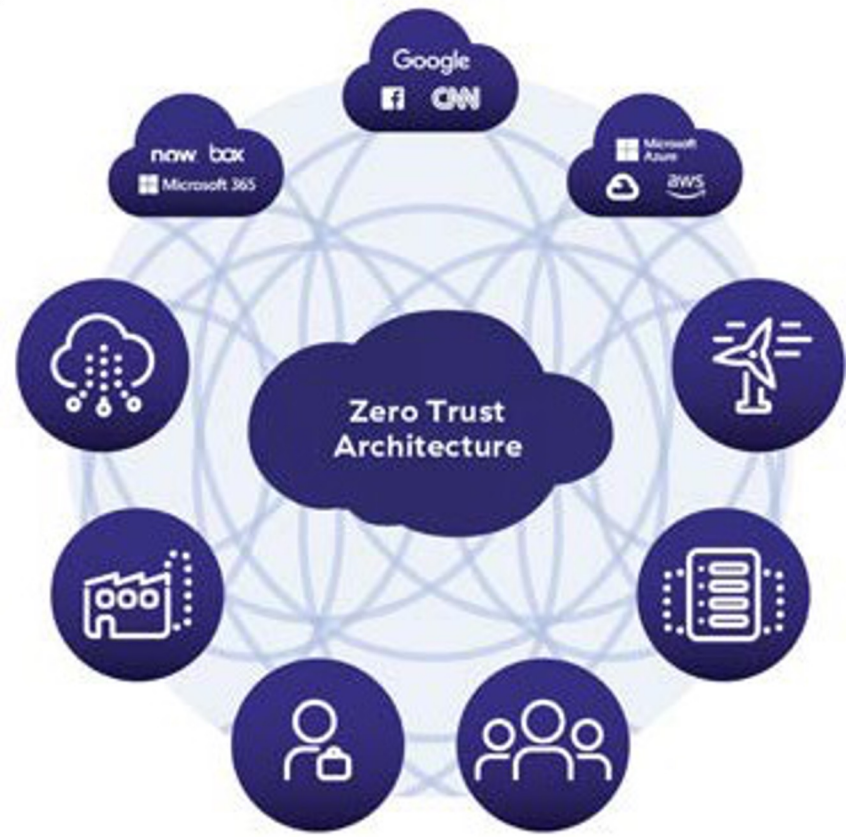


図19：ゼロトラスト・アーキテクチャー（ZTA）は、攻撃対象領域や水平方向への移動リスクを減らし、安全な方法でユーザーを必要なリソースに接続する。

そして、リクエストしたユーザーが職務の範囲外のことを要求していないかなど、リクエストのリスクを評価し、リスクを低減するためのコントロールを自動的に行います。過度にリスクの高いユーザーはブロックされる場合もあります。

次に、ビジネスポリシーに基づいて、組織が許可したアプリケーションにのみユーザーを接続することで、ポリシーの適用を行います（例えば、人事部門の社員だけにWorkdayのアクセスを許可し、営業部門の社員には許可をしないなど）。ZTAはこれらのリクエストすべてに対してポリシーを適用するため、他のアプリケーションやデータへの水平展開のリスクはなくなります。ネットワークのセグメンテーションを行う際によく発生する問題は、ユーザーとアプリケーション間のレベルでモニタリングが行われることで解消されました。

図20：ゼロトラスト・アーキテクチャー（ZTA）がサイバー侵害のリスクを減らすため、ユーザーを接続する前に取るステップ。

最後に、ZTAは、データセンターやパブリッククラウド環境からゼロトラストクラウドへのアウトバウンド方向での通信のトンネルを事前に作成しておき、そのトンネルの中に要求されたリソースへの安全な通信を確立します。接続がアウトバウンド方向であることは、ゼロトラストクラウド側からデータセンター・パブリッククラウド内の「信頼している」ネットワークへのインバウンド方向の入口をインターネットに晒す必要がないということであり、その結果、信頼しているネットワーク上に作成されているアプリケーションおよび、データのトランザクションはインターネット側からは隠されており、攻撃対象領域を生み出しません。適切に設計されたゼロトラスト・アーキテクチャーは、ユーザーも気づかないうちに、すべてのトランザクション（多くの場合、1日に数十億）に対してこれらのアクションを実行することができます。

ステップ2で挙げた企業での窃盗の例と比較すると、ゼロトラスト・アーキテクチャーの場合、大きく異なる結果になります。

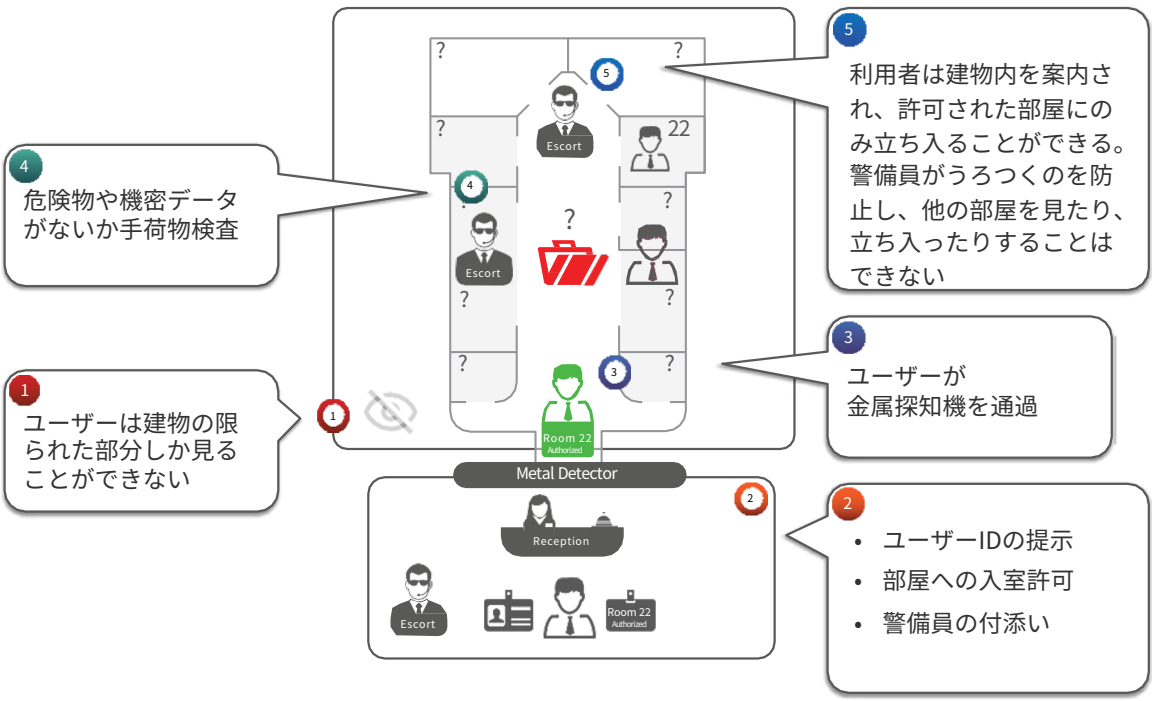


図21：ゼロトラスト・アーキテクチャーが防ぐ企業での盗難。

ゼロトラストは単なるテクノロジーではなく、戦略でありフレームワークです。これは様々な分野に浸透している新しい考え方であり、ゼロトラストを核としたソリューションを構築したベンダーにより実践的に実装されています。前セクションで説明したのは、まさにそのことです。

この技術を導入することで、ゼロトラストの原則に基づき、ユーザー、モノ、ワークロードが安全にパブリックまたはプライベートの宛先へアクセスできる基盤が整備されます。

ステップ2で説明したリスクの4つの分野に焦点を当てると、ゼロトラストは以下の点で有用です。

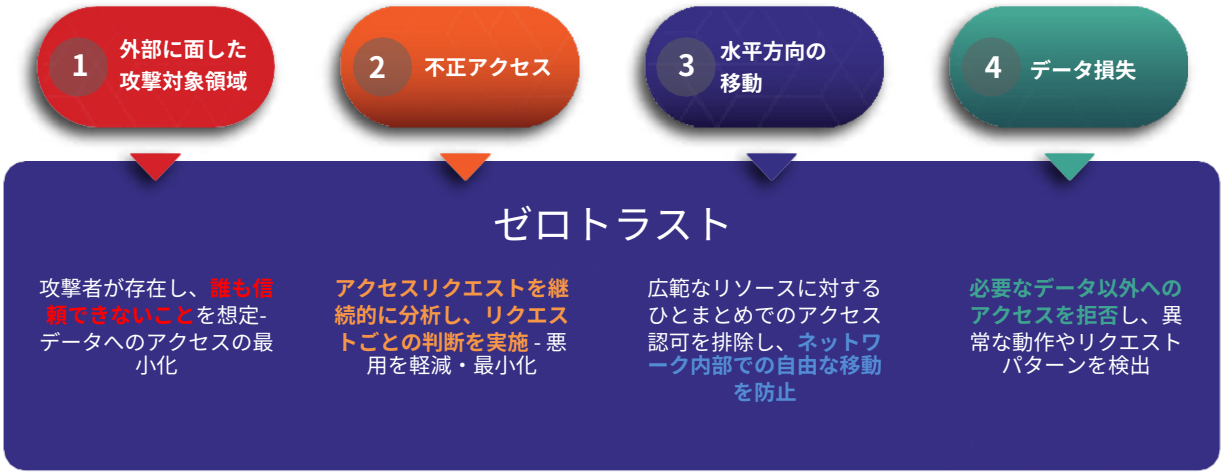


図22：ゼロトラストがサイバー侵害を防ぐ4つの方法

ゼロトラストはすでに多くの組織に大きな影響を与えています。パンデミックによって従業員が在宅勤務に移行し、ビジネスネットワークが拡大し、ITリソースに負荷がかかり、新たなサイバー攻撃のリスクが高まった時には、特に大きな価値を発揮しました。ZTAに移行した組織は、このような大規模な勤務形態の変化に伴うよくある問題や、セキュリティ上の懸念を回避しながら、従業員が自宅からシームレスにアクセスできるようにすることができました。とはいえ、多くの組織はまだ変革の過程のさまざまな段階にあります。

ゼロトラスト・アーキテクチャーは、米国政府機関NIST（800-207）、サイバーセキュリティ・インフラストラクチャ・セキュリティ庁（CISA）（ゼロトラスト成熟度モデル）、国防総省（DoD

セキュア デジタル トランスフォーメーションを ゼロトラストでいかに推進したか

- NOV社 CIO Alex Philips氏 (www.nov.com)

NOVのCIOである私の仕事は、ITインフラとセキュリティによって、我々のビジネスが世界を動かす人々の力になれるようにすることです。これは、60カ国にまたがる27,000人の従業員が、何千ものパートナー企業、サプライヤー、顧客と連携しているということを意味します。彼らは皆、いつでも、どこでも、どんなデバイスでも、安全に、そして信頼して利用できるテクノロジーを必要としています。過去数年間、私はNOVが、与えられた課題へより俊敏かつ柔軟に対応できるよう、セキュア デジタル トランスフォーメーションを主導してきました。

そのためには、コストを削減し、セキュリティを向上させ、ユーザーとIT管理者の双方を楽にする必要がありました。つまり、ゼロトラストへの移行です。我々は「信頼せず、常に検証する」という原則に従いたかったのですが、後にこれがゼロトラスト・アーキテクチャーと呼ばれるものだと知りました。これにより、隠れた脅威を検出してブロックする検査機能を利用することができ、私たちのリスク管理体制は大幅に改善されました。

セキュア デジタル トランスフォーメーションにより、NOVのビジネスはより俊敏になりました。数百万ドルを節約し、ユーザーの生産性を向上させ、サイバーリスクを低減できました。

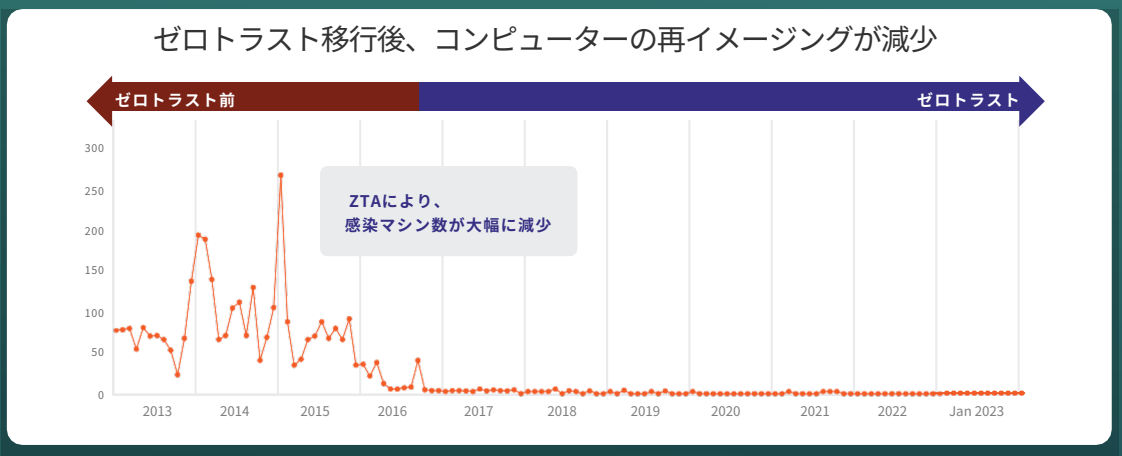


図23： NOVではゼロトラストへの移行後、コンピューターの再イメージング数が減少した。

）（ゼロトラスト・リファレンス・アーキテクチャー）、さらに大統領令（国家のサイバーセキュリティの向上に関する大統領令）、その他多数の世界的組織によって推奨されており、さらに、 Gartner、IDC、Forresterといったアナリスト企業からも支持を受けています。

ゼロトラスト・アーキテクチャーは、米国政府機関NIST、CISA、DoDや大統領の大統領令によって推奨されています。

この支持の高まりは、従来のアーキテクチャーが抱える課題と、それらの課題を軽減するゼロトラストの能力が認められていることを反映しています。そのため、企業やその取締役会、特に政府と取引する組織は、こうした傾向に特に注目しておく必要があります。

この傾向が顕著になっている分野のひとつが、サイバー保険です。保険会社は、組織のサイバーリスクモデルとポリシーの成熟度を評価するための指標となるデータをより強く求めるようになっています。ゼロトラストを採用することで、攻撃対象領域の減少に関する実証的データを保険会社に提供し、これらの技術が導入されていない場合よりもリスクが低く、管理が優れており、請求と損失がより少ない組織であろうことを示すことができます。

ゼロトラスト・アーキテクチャーには、上述のセキュリティ管理体制の強化に加え、技術コストの最適化、運用効率の向上、ユーザーエクスペリエンスの改善、合併・買収・分割（M&AD）の合理化、持続可能性の向上など、多くのビジネス上のメリットもあります。

ゼロトラストへの移行には、従来のネットワーキングとセキュリティの見直しが必要であり、この方向へとリーダーシップを発揮して議論を進められるかは、取締役会次第です。

セキュリティ体制とコンプライアンスの強化

不完全あるいは負担の大きいセキュリティおよびコンプライアンスの実践/構成は、ランサムウェア、マルウェア、ウイルス、フィッシング、コンプライアンス違反のリスクを高める。

効果の例

85%
ランサムウェア、フィッシング、その他のマルウェア/ウイルスの**被害減少**

25%
データ漏洩リスクの**低減**

ITコストの最適化

- インターネット/セキュリティアプライアンスの簡素化
- ハードウェアの容量計画/更新の削減/廃止
- ネットワークの簡素化/ローカルインターネットブレイクアウト

効果の例

75%
ハードウェアアプライアンスの**コスト削減**

50%
ネットワーク費用の**削減**

ユーザーエクスペリエンス

- ネットワークへのヘアピン接続（データセンターへ全ての通信を一旦集約させる）の廃止による通信遅延の削減
- 帯域制御による重要アプリの優先順位付け
- M365とその他SaaSの最適化

効果の例

30-40%
インバウンド/アウトバウンドトランザクションの**待ち時間削減**（ユーザーの生産的時間）

業務効率化

故障/障害対応、OS/ファームウェアのアップデート、パッチ適用、リフレッシュ・サイクル、変更管理のスケジューリング等に費やしていた正社員の作業時間の最適化と、契約社員の人件費の削減。

効果の例

50%
インバウンド/アウトバウンドのインターネット・セキュリティ・アプライアンス（新規および既存拠点）の**管理労力削減**

合併・買収

- M&Aの推進
- セキュリティ面でのアクセス権やポリシーの評価を含めた、買収先企業の従業員の迅速な配属（オンボーディング）

効果の例

2-3X
M&Aシナジー創出までの時間**短縮**
UXと生産性の**向上**
セキュリティ体制の**向上**

サステナビリティ／二酸化炭素排出量

- ESG（環境、社会、ガバナンス）活動、レポーティング、スコアの向上

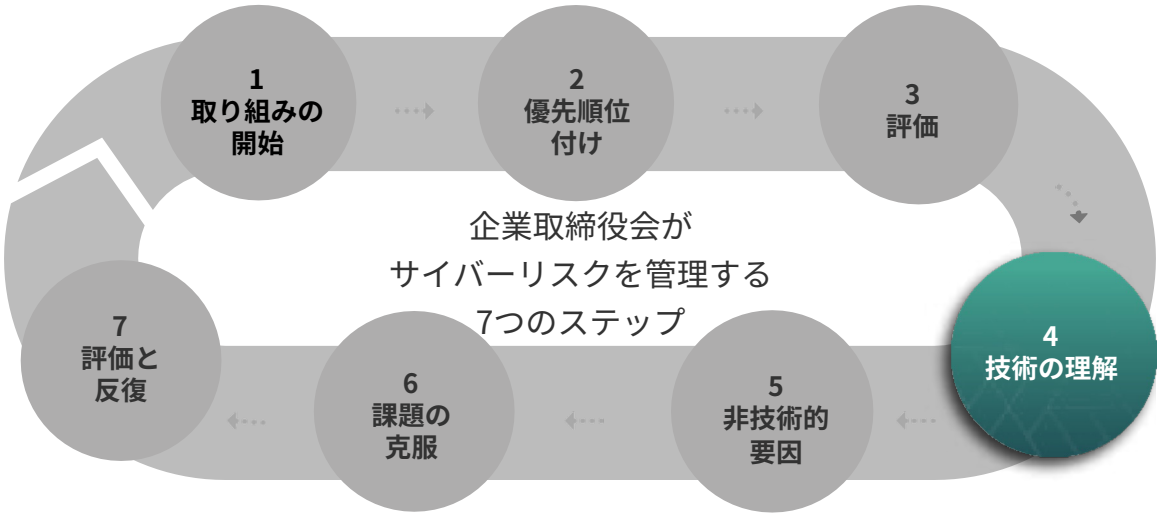
効果の例

50%
電力使用効率 (PUE)の改善：出荷、入荷、交換部品の削減

電力と冷房によるCO2排出量
削減

図24：ゼロトラスト・アーキテクチャーは、幅広い経営効果をもたらす。

キーポイント:



- 組織の保護すべき最も重要な資産（クラウンジュエル、王冠の宝石）の見極めと、サイバーセキュリティ戦略の優先順位付けを支援することが重要である。
- 組織は、大きなサイバーリスクをもたらす暗黙の信頼モデルから脱却するために、ゼロトラスト・アーキテクチャー（ZTA）を採用している。ZTAは、ユーザーとデバイスを検証し、リスクを評価し、ポリシーを適用し、安全な接続を確立する。
- ZTAの利点は、外部に公開された攻撃対象領域を減らし、ネットワーク内部での水平方向の移動を阻止し、データ損失を防ぎ、侵害による被害を最小限に抑えることである。ZTAはセキュリティをWork-From-Anywhere（自宅を含め、どこからでも仕事ができる）やクラウドに順応させる。ゼロトラストは、リスク、コスト、ユーザビリティの3つの側面での改善をもたらす。
- ZTAは、セキュリティを向上させる手段として政府やアナリストに支持されている。また、サイバー保険における組織の評価を高めることにもつながる。
- 取締役会は、サイバーリスクを最小化するために、ゼロトラストのフレームワークとテクノロジーを採用するよう、組織内での議論を促進すべきである。

非技術的要因への取り組み

マインドセット、スキルセット、プロセス、組織

なぜこのステップが重要なのか？

サイバーリスク管理に取り組む際、課題の技術的な側面だけに注目しそうになることがあります。デジタルトランスフォーメーションを、問題「Y」を解決するためにテクノロジー「X」を導入することと捉え、変革がもたらす非技術的な影響を無視しがちです。組織の変革を成功に導くには、いくつかの非技術的要素も重要であり、それらを見逃すと大きなリスクや損失を招く可能性があります。

取締役会は何をすべきか？

あなたや他の取締役には、テクノロジー以外の要因（非技術的要因）をしっかりと考慮し、対処する役割があります。適切なテクノロジーの採用と同様に、セキュリティ対策を頓挫させる可能性のある要因を積極的に管理することも重要です。組織文化／マインドセット、取締役会／従業員のスキルセット、プロセス、組織構造は、テクノロジーやセキュリティの取り組みの成果に大きく影響するものであり、サイバーリスクを管理する上で不可欠な要素だからです。

図25： サイバーリスク管理の成功は、いくつかの非技術的要素に依存している。

組織文化とマインドセットの変革

変革の取り組みが組織の文化によって歓迎されない場合、成功への道は険しいものになります。特にサイバーセキュリティにおいては、人間の行動に起因するサイバーリスクを効果的に削減するために、人々の協力が必要です。新たなセキュリティ対策に不満を持つ従業員は、プロセスを無視したり、許可されていないショートカットを作成したり、承認された方法以外で作業したりする可能性があるからです。

取締役会の一員であるあなたは、組織の文化や考え方を変える上で大きな影響力を持っています。あなたが積極的に変化を支持し、推進することで、他のメンバーもそれに追随するようになります。

ゼロトラスト・プラットフォームへの移行など、セキュリティの抜本的な見直しを組織のリーダーに納得してもらうためには、まず言葉選びや表現方法に気を遣う必要があります。従業員はサイバーセキュリティの話題に否定的な反応を示すことが多くあります。セキュリティ対策は、生産性を妨げる障害物や、実際の業務に取り掛かる前の煩わしい一手間として広く認識されているからです。支持を得るためには、経営陣が、ゼロトラストの取り組みの目標はビジネスの円滑化の促進であり、業務の流れを妨げることではないことを強調することが重要です。

取締役会の一員であるあなたは、組織の文化や考え方を変える上で大きな影響力を持っています。声に出して変革を奨励することで、後に続くよう皆に勇気づけることができます。

例えば、セキュリティに関する会話を、ルールベースから、リスクベースに変えていくことは、ベストプラクティスのひとつです。言い換えると、CISO/CIO/CROなどのセキュリティリーダーに対して、業務プロセスに関する議論の際に「それはやってはいけません」と言う代わりに、リスクを考慮した別の（改善された）方法でどのようにタスクを実行するか、例示するように奨励します。ビジネスのミッションとユーザーにとってのメリットを議論の中心にすることがカギとなります。

また、工場、医療機器、スマート家電などの運用技術（OT）を議論に含めることも重要です。これによりあなたが持つセキュリティ懸念の対象範囲の広さを示すことで、ユーザーに直接的な影響が出る範囲のみならず、より広い視野を変革のゴールとして見ていることを強調します。

先進的なセキュリティへの考え方、技術的な知識、サイバーリスクの低減への熱意をあなたが例示することで、組織のリーダーに変革を成功させる力を与えることができるでしょう。

プロセスの最適化

組織のサイバーリスクを効果的に低減するためには、運用を管理する新しいプロセスと、インシデント対応の方法を理解することが求められます。

自己評価または第三者の評価に基づいて、プロセスの成熟度の把握をすることは、リスク低減にとって必須です（ステップ 3を参照）。

サイバーリスクの態勢を改善するには、組織の内部プロセスの刷新が必要であり、あなたはそのために重要な役割を果たすことができます。

サイバーリスク管理体制を改善するには、組織内のプロセスの刷新が必要であり、あなたはその実現を確実にするための主要な役割を果たすことができます。組織には、あなたが見直しが必要と感じるかもしれない手作業でのリスク管理プロセスが数多くあります。成功するサイバーセキュリティ・プロセスのフレームワークの基礎を築くには、いくつかの要件があります。

- **定期的なリスク評価** - 取締役会は、組織のCISOまたは適格なサードパーティベンダーから定期的にリスク評価を受けるプロセスを確立すべきである。
- **継続的なサイバーセキュリティ研修** - 取締役会は、取締役会自身が継続的な研修を確実に与えられるためのプロセスを確立すべきである。
- **インシデント対応マニュアル** - 取締役会は、政府当局、場合によってはメディアを含む利害関係者にインシデントの発生を伝達する際の計画を立てておくべきである。（米国では、SEC の新ガイドラインが、公開企業の重大な違反の報告に関する厳格な規則を定めている。）

- **定期的な報告** - 取締役会は、インシデントや、サイバーリスク管理体制の変更などについての報告が、組織幹部によって適時に伝達されるプロセスを確立すべきである。（米国の公開企業では、 SECの定めたルールの一部として、サイバーリスクを評価・管理するためのプロセスに関する定期的な開示が求められている。）

ゼロトラスト・アーキテクチャーを採用することで、従来型のプロセスが生み出すリスクを最小限に抑えることができます。不要なハードウェアを取り除き、冗長なセキュリティ管理を廃止し、通信の保護を集中管理することで、複雑さを大幅に軽減します。 このような改善は、プロセス改善のさまざまな分野に広く影響しますが、中でもM&Aに伴う統合に大きな影響を与えます。

取締役会の一員であるあなたは、M&Aに関わる機会も多いでしょう。異なる企業のネットワークと、それに付随するセキュリティ機能をうまく統合することは、ITチームにとっては悪夢です。そしてその過程では、業務を軌道に乗せるために、セキュリティ面での妥協が数えきれないほどなされます。生産性のためにセキュリティを犠牲にする場合、それに伴って増加するサイバーリスクの対応にかなりの時間を費やす必要があります。

ゼロトラスト・アーキテクチャーを採用することで、従来型のプロセスが生み出すリスクを最小限に抑えることができます。不要なハードウェアや、必要以上に冗長なセキュリティ管理機能を廃止し、通信の保護を集中管理することで、複雑さを大幅に軽減します。

ゼロトラストは、M&Aに伴う統合プロセスを大幅に簡素化し、統合にかかる時間と価値実現までの時間を大幅に短縮します。

そして、組織の防御力を低下させることなく買収を達成することができます。また、事業分割にもゼロトラストは適用できます。（訳注: 同一物理ネットワークの中で、論理的にネットワークを分割もしくは物理的にネットワークを分割した上で、必要な通信のみをM&Aと同様に許可する

ことができる。そうすることで、必要な通信の確保及び遮断すべき通信の遮断を適切に行うことができる。）アプリケーションやデータへの必要なアクセスを継続して提供できることで、移行期間中のサービス提供契約（Transition Service Agreement)に沿って分割された事業を円滑に継続できるようにします。

スキルセットの適応

ベストプラクティスは、取締役会の一部または全員が以下の5つのスキルを有していることです。

1. 適切な質問をするために必要な、サイバーの世界に関する課題やリスクの管理についての理解
2. 規制要件に対しての意識
3. 業界標準とベストプラクティスに関する精通
4. インシデント対応とインシデント発生時の事業継続策についての理解
5. サイバーセキュリティガバナンス（統治）に関する知識

サイバーセキュリティのトピックに関する直接的な知識を持ったメンバーがいない取締役会においては、サイバーセキュリティ担当部署が報告するリスク要因が過多になる傾向があります。

サイバーリスクを理解し対処するためのスキルセットは、大規模な組織でも必要です。リスク低減の目標達成に必要な、従業員へのサイバーセキュリティに関する教育レベルを決定するにあたり、あなたの役割が重要となります。取締役会が監督を行うべき具体的なグループは以下の通りです。

- 組織内のCレベルのリーダー（経営幹部）
- IT部門
- 一般社員

経営幹部のスキルセットを見ることで、革新的で先進的なセキュリティリーダー、特に変革を推進する知識と信念を備えたセキュリティリーダーを組織に採用するための要件を明確にする手助けをすることができます。

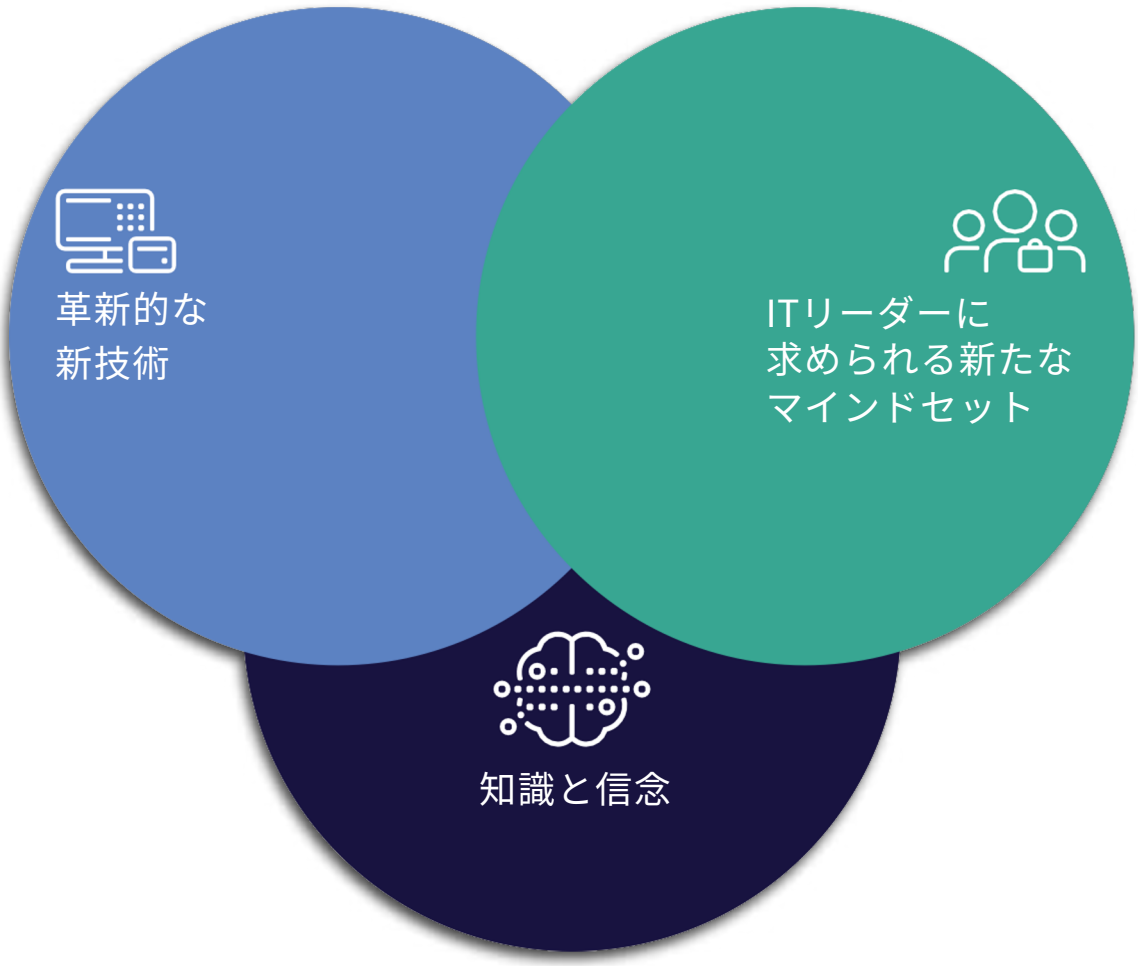


図 26：セキュリティに関する議論をビジネスリスクとイネーブルメントの観点から再構成することで、考え方を変える

技術に対する進歩的マインドセットについて適切な質問をすることや、ゼロトラストのような新技術に関する高度な知識を有していることは、ITリーダーに必要なマインドセットや知識・信念とともに、変革を推進する上で強力な組み合わせとなります。

テクノロジーをクラウドベースのゼロトラスト・アーキテクチャーと置き換えることで、組織のIT部門は特定のベンダーにのみ通用するスキルを必要としなくなります。代わりに、技術者は新たな環境に関連するスキルを身につける必要があります。

幸い、ITプロフェッショナルの多くは、変化する技術的な需要に適応することに慣れており、必要に応じて再スキルアップすることに意欲的です。また、あなたの組織が、新技術の導入に合わせて、IT人材のスキルアップにも投資しているかどうかを問いかけることで、積極的なアプローチを取ることも有効です。

最後に、取締役会の役割として、組織の従業員に対する一般的な教育の重要性を認識しておく必要があります。サイバー攻撃の最も一般的かつ成功している手法は、従業員を騙すことです。会社の全従業員のサイバー意識を向上させることは、リスク削減という莫大な見返りをもたらすものであり、最優先事項とするべきです。

サイバー攻撃の最も一般的かつ成功している形態は、従業員を騙すことです。会社の全従業員のサイバー意識を向上させることは、リスク削減という莫大な見返りをもたらすものであり、最優先事項でなければなりません。

したがって、従業員が用心深くあり、意識付けされており、気づきを恐れず報告することを実現するためには、目標設定、推奨される行動、インセンティブを経営幹部が揃えることが重要です。

組織的課題の克服

IT部門の構造がサイロ化している場合、ゼロトラストを採用する際に特有の課題を引き起こす可能性があります。多くの場合、各部門にはアプリケーション、ネットワーク、セキュリティなど特定のIT機能に沿った役割があり、このような区分は組織図にマッピングする上では理にかなっていますが、実際には曖昧さや問題を引き起こすことがあります。例えば、クラウドアプリの動作が遅い場合、それは誰の責任なのでしょうか？従業員が新しい携帯電話で仕事のメールをチェックできない場合、それはアプリのせいなのか、ネットワークのせいなのか、それともセキュリティのせいでしょうか？組織がこのような問題に対処し、責任の所在を明確化する方法は数多くありますが、標準化されたアプローチは存在しません。

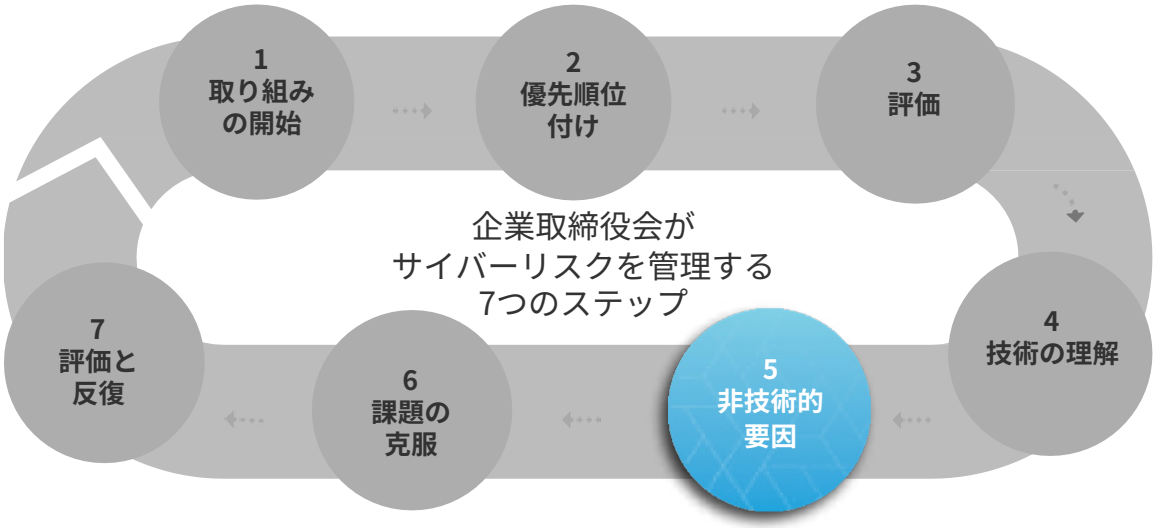
IT部門のサイロ化が引き起こす問題は、大規模な技術的取り組みが進行している時ほど深刻化します。しかしそこでゼロトラスト・フレームワークが正しく機能すれば、ネットワーク・チーム、セキュリティ・チーム、エンドポイント・チームだけでなく、経営幹部も積極的に関与するため連携が促進され、役割の曖昧さを解消するための優れたソリューションとなります。上級幹部たちが、サイバーリスク最小化のために必要な変化を推進するよう促すことが取締役会にとっては重要です。これにはサイロ化を解消し、連携を推進することも含まれます。

あなたの配下の幹部たちは、セキュリティ変革後の役割分担の曖昧さを避けるために、以下のような問いかけをすべきです。

- アクセスポリシーの設定と管理は誰の責任か？
- 安全な接続の維持は誰の責任か？
- セキュリティポリシーの設定と管理は誰の責任か？
- ユーザー・アクセスポリシーが最新の状態であること、また、権限が付与されたまま積み上げられていくのではないことを確認するのは誰の責任か？
- ユーザー、デバイス、およびアカウントが一貫してゼロトラストのポリシーと手順に準拠していることを確認するのは誰の責任か？

これらの役割のいくつかは、サイロ化した技術部門のメンバー間の相互協力が必要になる可能性があります。例えば、アプリケーション・チームとセキュリティ・チームのメンバーが協力してユーザー・アクセスポリシーを作成し、クラウド環境で展開する必要があるかもしれません。しかし、誰が何を担当するかを事前に把握してあれば、関係者全員にとって移行が容易になります。取締役会のメンバーは、従来の「サイロ化した」IT組織における相互協力、または役割の曖昧さを徹底的に解消した、新しい組織構造の構築を推進すべきです。

キーポイント:



- サイバーリスクの管理においては、非技術的要因も技術的要因と同等に重要である。
- 組織文化とマインドセットの変革が重要であるため、ビジネスリスクの低減とビジネスのイネーブルメントを中心とした議論に再構成することで、セキュリティ変革を組み込むことも有効である。
- プロセス最適化の監督とは、成熟度レベルの理解、定期的な評価の実施、トレーニングの確実な実施、インシデント対応手順の作成、定期的な報告を意味する。
- スキルセットの調整を監督することで、取締役や経営幹部が必要なスキルを身につけられるようにするだけでなく、ITスタッフの再教育や全従業員の教育も行う。
- 組織の課題（IT部門のサイロ化）の解決を監督することで、相互協力を促進し、ゼロトラストのような取り組みにおける各部門の責任を明確にする。

課題の克服

サイバーセキュリティの変革を監督する上での障害となりうる要素

なぜこのステップが重要なのか？

取締役会のメンバーが組織のサイバーセキュリティ変革を推進する際、他の大規模な変革の取り組みを監督する際と同様に、さまざまな課題に直面する可能性があります。これらの一般的な課題に対し、取締役会レベルで対処しなければ、サイバー関連の取り組みにおける組織のタイム・トゥ・バリュー（価値実現までの時間）を遅らせる可能性があります。

取締役会は何をすべきか？

サイバーセキュリティ変革による変化が組織にもたらす多くの一般的な課題は、トレーニングや教育、また、取締役会全体に責任を分散させた監督プロセスに、最小限の変更を加えることで対処することができます。

図27： 取締役会がしばしば直面する6つの一般的な課題

取締役レベルのサイバー専門知識の不足

多くの取締役会は、通常、非技術的な経歴を持つメンバーで構成されているため、サイバーセキュリティに関する経験が不足していることがあります。そのため、サイバー関連事項に関する監督や関与、特に関連リスクの理解や提言が難しくなっています。

組織のサイバーセキュリティを真に把握するには、以下の組み合わせが必要です：

- 組織のサイバーセキュリティ戦略とサイバー脅威の状況を理解する
- 組織のサイバー関連の欠点と脆弱性を理解する
- 大きく変化し続ける外部脅威を評価するための明確なベースラインを持つ

CISO/CIO/CROや、サイバー関連の取り組みに関与する他の経営幹部と話し合う時間を確保することで、このような知識の大部分を得ることができます。その際、サイバーセキュリティ戦略の全体像と組織内に存在するギャップに関する説明は、エンタープライズリスク、重大度合い、損失の観点での注力点とともに提示されると特に有益です。また、中立的な外部の専門家の知見からは、 CISOからのブリーフィングで得られるサイバー関連の洞察とはまた違った知識が得られます。取締役会を対象としたサイバー関連のトレーニングや認定取得も、セキュリティの概念を理解するための強力な基盤を作ります。サイバーセキュリティの話題を扱う、独立したニュースソースをチェックすることも、この領域をより良く理解するために役立ちます。

取締役会を対象に、サイバー分野に関する研修や認定取得を行うことで、セキュリティの概念を理解するための強固な基礎を築くことができます。

取締役会のサイバー専門家不足への取り組み

CAP Groupによる最近の調査[16]では、Russell 3000に選出されている企業の90%において、サイバーセキュリティの専門知識を持つ取締役が1人もいないことが明らかになり、役員レベルの人材における専門知識の不足が顕著であることが浮き彫りになりました。

しかし、その傾向は変わりつつあります。2021年には、新しい取締役を任命したFortune 500企業449社のうち17%がサイバーセキュリティの経験者を選び、2020年のわずか8%から上昇しました。('Heidrick & Struggles' Board Monitor.17を参照）。

複雑なサイバー脅威の状況に対する不十分な理解

サイバー脅威の状況は常に変化しており、取締役会が最新の脅威や傾向に対応することは困難です。サイバーリスクと、リスクが組織へ及ぼす影響を真に管理するためには、サイバーリスク管理対策と監視体制を継続的に改善していかなければならないというのが現実です。取締役会は、変化し続けるサイバー脅威に対し、自組織がどのように適応できるかについて、強い自信を持つ必要があります。

どこに脆弱性が存在し、リスク低減にはどのような取り組みが必要かを取締役会が明確に理解する必要があるという期待値をCISOと共有しましょう。これによって、変革に必要な経営幹部からの支持を得ることができます。具体的なビジネスへの影響が明確になっているサイバー脅威に対して、経営幹部が注意を払う可能性が高まります。取締役会が、緊急性と関心を取締役会全体と経営陣に喚起することで、組織がサイバーリスク変革の取り組みにより高い優先順位を

16 (2023, June 6). CISOs as Board Directors. CAP Group. https://www.thecap.group/post/ cisos-as-board-directors
17 (2022, June 6). Cybersecurity expertise creeps onto Fortune 500 boards. CIOdive.com. https://www.ciodive.com/news/fortune-500-boards-cybersecurity/626650/

つけるよう、影響を与えることができます。これは、一般的にCISOによって提起される、既知の大きなサイバー脅威の解決につながります。

サイバーセキュリティに割けるリソースが限られている

役員は、サイバーセキュリティの議論に時間と関心を割くことが難しいと感じるかもしれません。その結果、他のリーダーシップ層が包括的なサイバーセキュリティ対策に組織として注力するよう促すことが困難になることがあります。

しかし、サイバー攻撃が成功した場合に発生しうる損害を考えれば、セキュリティ問題は取締役会での定期的な議題にする必要があります。このような協議には、監査・リスク分科委員会（または同等のグループ）からの定期的な最新情報を含めるべきです。組織におけるサイバーの現状を把握する一貫した方法を持たないことは、サイバー攻撃事案が事業運営、財務安定性、ブランドの評判に及ぼす包括的な影響を考えると、非常に危険なことです。

サイバーアップデートの効果を最大化するため、取締役会に提出する報告書は、最も重要な問題に焦点を当てるようします。アップデートは以下の点をカバーする必要があります:

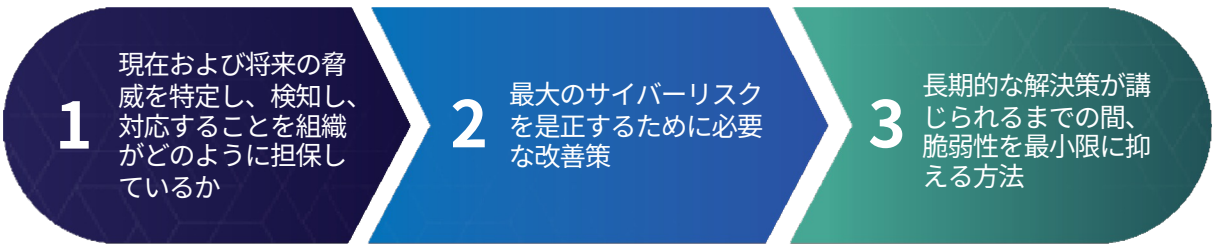


図28： 取締役会のメンバーは、経営陣からの次のような最新情報を得るべきである。

監査委員会およびリスク委員会に所属する取締役会メンバーは、組織のサイバーセキュリティリスクとニーズに関する情報を取締役会のより広い範囲に周知することで、注意を向けるべきです。例えば、取締役会は、組織がサイバーインシデントに対して財務的な備えができていると自信を持って言えるでしょうか？

主要な事業革新や成長への取り組みについて、潜在的なサイバーセキュリティリスクがないか検証されているでしょうか？ 取締役会は、提供されるべきサイバー関連の最新情報とその提供方法について基準を設定することで、サイバーへの意識をプロセスに適切に組み込むことができます。また、取締役会への報告書にサイバーリスクに関する検討事項を盛り込むことで、取締役会に持ち込まれる前にサイバーセキュリティが考慮されるようになります。

サイバーセキュリティの有効性に関する全体的な可視性の欠如

いかなる取締役会も、組織のサイバーセキュリティの有効性を完全に可視化することはできませんが、CISOと定期的にやりとりし、外部からの評価を受けることで、より良い可視性を得ることができます。 CISOから組織のサイバーセキュリティ・プロセスの全体像について説明を受けることで、取り組みの現状と将来に対する自信がさらに深まります。

また、定期的にCISOとの時間を取り、どこに重点を置いているかを説明してもらいましょう。サイバーセキュリティの専門家の半数以上（51%[18]）が、仕事のストレスや仕事の課題によって夜も眠れない状態になっています。CISOは、脅威から脅威へ、ギャップからギャップへと絶えず移行しながら、その阻止と対処に全力で取り組んでいるため、組織のサイバー・ポジションを俯瞰的に見ることができない可能性があります。正しくサイバーリスク管理体制の評価を実施するために時間を割くよう、取締役として組織に促すことは、多くの企業にとって、新たな課題を発見し、エンタープライズリスクとして現在のサイバーリスクを再定義するためのベストプラクティスとなっています。

取締役会メンバーが、サイバーリスク管理体制の徹底した評価に時間をかけるよう組織に促すことは、多くの企業にとって、新たな課題を発見し、エンタープライズリスクに関連する現在のサイバーリスクを見直すためのベストプラクティスとなっています。

18 (2021, September 8). Stress and Burnout Affecting Majority of Cybersecurity Professionals. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/stress-burnout-cybersecurity/

サードパーティリスクに関する理解不足

サードパーティの個人、ベンダー、パートナー企業に関連するリスクは、現在および将来のサイバー状況を把握する際に、見落とされがちであったり、誤って低リスクのカテゴリーに分類されることさえあります。

多くの組織では、重要なサービスをサードパーティに依存していますが、このような関係に関連するサイバーセキュリティ上のリスクについて、取締役会が適切に管理することは困難です。組織外の関係者は、組織にとって最大のサイバー脅威のひとつであり、その脆弱性は組織のコントロールの及ばないところにあります。

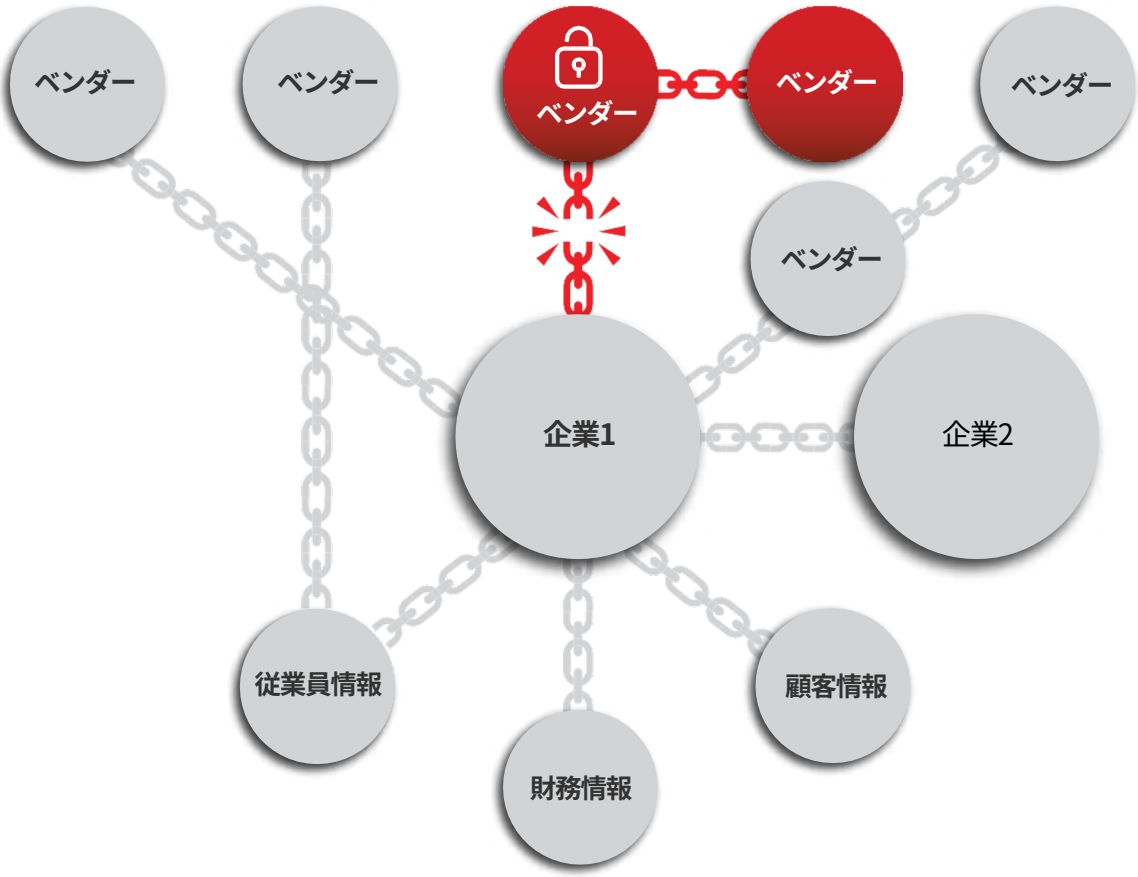


図29： ベンダーのようなサードパーティによってもたらされるリスクは、取締役会や経営陣の手に負えない問題を引き起こす可能性がある。

大きく報道されたSolarWinds社のハッキング事件のように、サードパーティへの大規模なサイバー攻撃は、相互に接続された組織のエコシステム全体をダウンさせる可能性があります。[19]

サードパーティリスクには、組織のテクノロジーシステムや接続機器にアクセスできる外部の個人や組織が含まれます。他組織のサイバー体制を信頼することはできませんが、ベンダーのインフラへのアクセスを制限することはできます。情報やシステムへのアクセスを制御することで、攻撃者がサードパーティを介して組織に侵入するのを防ぎます。この概念は、ゼロトラスト戦略の基礎となる要素です。

他組織のサイバー体制を信用することはできませんが、ベンダーが貴社のインフラにアクセスするのを制限することは可能です。

取締役会での情報アップデート時に、サードパーティリスクについて質問し、議論を促すようにします。どのようなタイプの組織変革を行っていても、対処する必要があるサードパーティリスクを検討し、組織を保護するための措置を講じましょう。

法律および規制上のサイバー関連要求に対応することの複雑性

サイバーセキュリティの分野には関連する複雑な法律や規制があるため、取締役会が取り組みを監督するのは困難なことです。取締役会の平常時の責任範囲と、大規模なサイバー攻撃事案が発生した際の責任範囲を把握することも含め、それぞれの国や地域における法的責任を理解することが重要です。

19 TechTarget (2023, June 27). SolarWinds hack explained: Everything you need to know. WhatIs. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

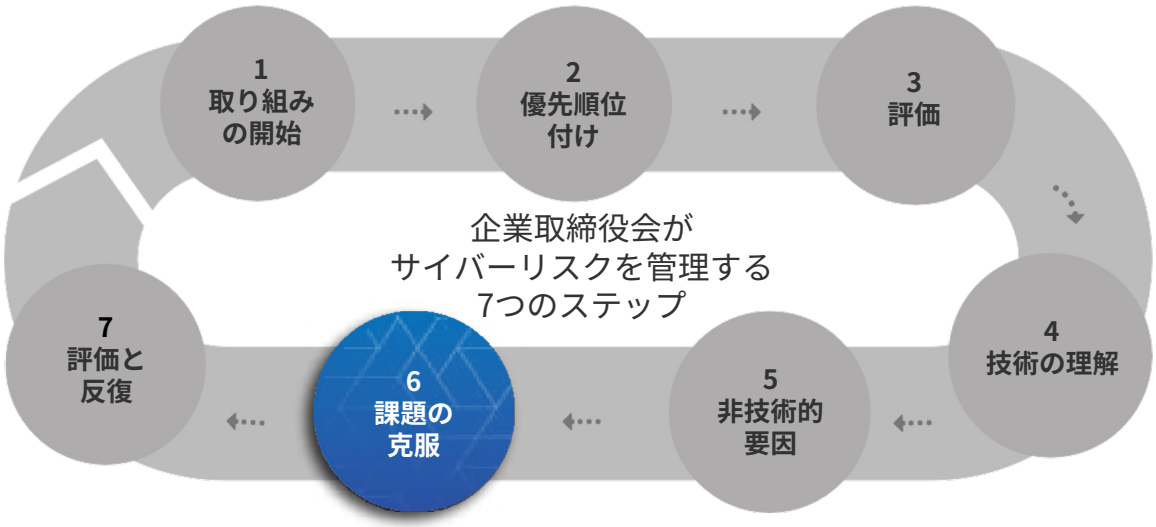
経営幹部と社内外の法務担当者が定期的に取締役会に法的義務を報告することで、サイバーに関する法規制の状況により適切に対処することができます。

組織に関連する、サイバーセキュリティおよび法に関する考慮事項を特定し対処するためには、取締役であるあなたの幅広い監督が不可欠です。サイバーリスクに関する変革では、このような法的義務や規制要件を満たせない場合、深刻な問題が発生する可能性があります。

経営陣全体でサイバーに対する意識を高め、各組織のサイロに対してトップダウンでサイバーセキュリティの考え方を推進できるようにしましょう。

取締役会にとってのベストプラクティスは、組織のサイバーリスクの主管者を明確に理解し、それがCISOだけの責任ではないことを確認することです。サイバーリスクは非常に重要であり、最終的にはCEOが責任を負いますが、その上で、CISO、CIO、CRO、その他の経営陣のメンバーに責任を委ねることができます。サイバーリスク管理の責任を分担している組織は、全体的なリスクをより前面に押し出し、サイバー変革に伴う説明責任を果たし、より強力な経営管理を行っています。経営陣全体でサイバーに対する意識を高め、各組織のサイロにトップダウンでサイバーセキュリティの考え方を推進できるようにしましょう。そうすることで、サイバー攻撃に対する耐性を向上させ、関連するビジネスリスクを最小限に抑えることができます。

キーポイント



- 取締役会にはサイバーセキュリティの専門知識が不足していることが多く、監督が難しくなっている。集中的なトレーニングや独立した情報源を活用することで、知識を深めることができる。
- 脅威の状況は急速に進化する。取締役会には、組織が新たな脅威に対応できるという自信が必要である。情報アップデートは重要な問題に焦点を当てるべきである。
- サイバーセキュリティは、定期的に取締役会の議題とすべきである。監査／リスク委員会は、取締役会にサイバーリスクについて報告する必要がある。
- 取締役会は、定期的な評価を行うことでサイバーリスクに対する理解を確認することができる。重点分野についてはCISOと定期的な確認を行う。
- 組織はサードパーティリスクを管理しなければならない。取締役会は、サイバーリスクに関する法的義務を理解し、リスクが組織全体で幅広く対処されていることを確認する。

評価と反復

効果分析と継続的改善

なぜこのステップが重要なのか？

サイバーリスク管理は継続的な取り組みであり、組織の変化、脅威の状況の進化、ビジネスニーズの変化などに応じて、ステップ1〜7を繰り返し実施します。ゼロトラストへの移行はサイバーリスクの最小化に向けた大きな一歩ですが、一度で完了するプロセスではありません。

取締役会は何をすべきか？

取締役会は、継続的にリスクを再評価し、技術的および非技術的要因に影響を与え、最終的に課題を克服し、その変化による影響を測定する必要があります。そして、あなたの組織がゼロトラストへの取り組みを開始したら、サイバーリスクの低減に関して達成したメリットを定量化する時です。

最も重要な指標は、なぜリスク軽減戦略を開始するのかを正当化することができる指標です。具体的な目標は組織によって異なりますが、出発点となる一般的な指標は、リスク削減、技術コスト削減、業務効率化に関する測定結果です。

具体的な目標は企業によって異なりますが、良いスタートポイントとなる共通の測定基準がいくつかあります。リスク削減、技術コスト削減、業務効率化などです。

リスク削減の効果を測定するには、以前のセキュリティ管理体制と現在のセキュリティ管理体制の有効性と適用範囲を比較します。変革の初期に作成された詳細なリスク評価表を参照し、各項目の現在の状況を評価します。ゼロトラストへの移行により、組織はランサムウェア、フィッシング攻撃、データ損失、内部者による脅威に対する強固な防御力を持つことになります。プラスの成果を見積もる際には、これらの各項目を検証し、定量化する必要があります。

組織が安全であり続けることで日々回避されている、多額のコストを見過ごさないことが重要です。データ漏洩に見舞われた組織が負う非金銭的な損失を考えてみましょう。これには、組織のイメージや評判へのダメージ、顧客の信頼の喪失、生産性の低下、データ関連の損害などがあります。例えば、重要な知的財産が盗まれた場合、組織は競争上の優位性を完全に失う可能性があります。顧客の個人データが盗まれた場合には、顧客基盤の回復は困難かもしれません。

侵害を回避するためのコストの見積もりに完璧な方程式はありません。しかし、考慮すべき事項としては、悪意によるサイバー攻撃事案に伴う時間当たりのコスト、ビジネス機会の損失、ブランドイメージへのダメージ、顧客離れなどが挙げられます。それらの事項から得られた概算値を、

サイバー攻撃が成功した場合の既知の平均コストに加えることで、侵害を回避することで節約できたコストを見積もることができます

また、サイバー攻撃が成功した場合、経営幹部の退職を招く可能性もあります（2022年の調査[20]によると、ITサイバーセキュリティ・リーダー全体の約3分の1）。中小企業（SMB）にとって、サイバー攻撃から受ける影響はより甚大で、Forbesによると、サイバー攻撃を受けてから6カ月以内に廃業する中小企業は60%[21]にも上っています。

侵害を回避するためのコストの見積もりに完璧な方程式はありません。しかし、悪意によるサイバー攻撃事案の時間当たりのコスト、ビジネスチャンスの損失、ブランドへのダメージ、顧客離れなどは考慮する必要があります。

20 TechTarget (2022, November 1). Nearly one-third of cybersecurity leaders have considered leaving their organizations. SC Media. https://www.scmagazine.com/news/nearly-one-third-of-cybersecurity-leaders-have-considered-leaving-organizations

21 (2022, August 16). Businesses Shutting Down Business. Forbes. https://www.forbes.com/sites/emilsayegh/2022/08/16/businesses-shutting-down-business/?sh=22d90a764cc6

サイバーリスクが与える財務的影響と ゼロトラスト移行のメリットの計算

第三者機関では、ビジネスリスクとゼロトラスト・トランスフォーメーションの効果を算出するために、しばしば6段階の方法論を用います。

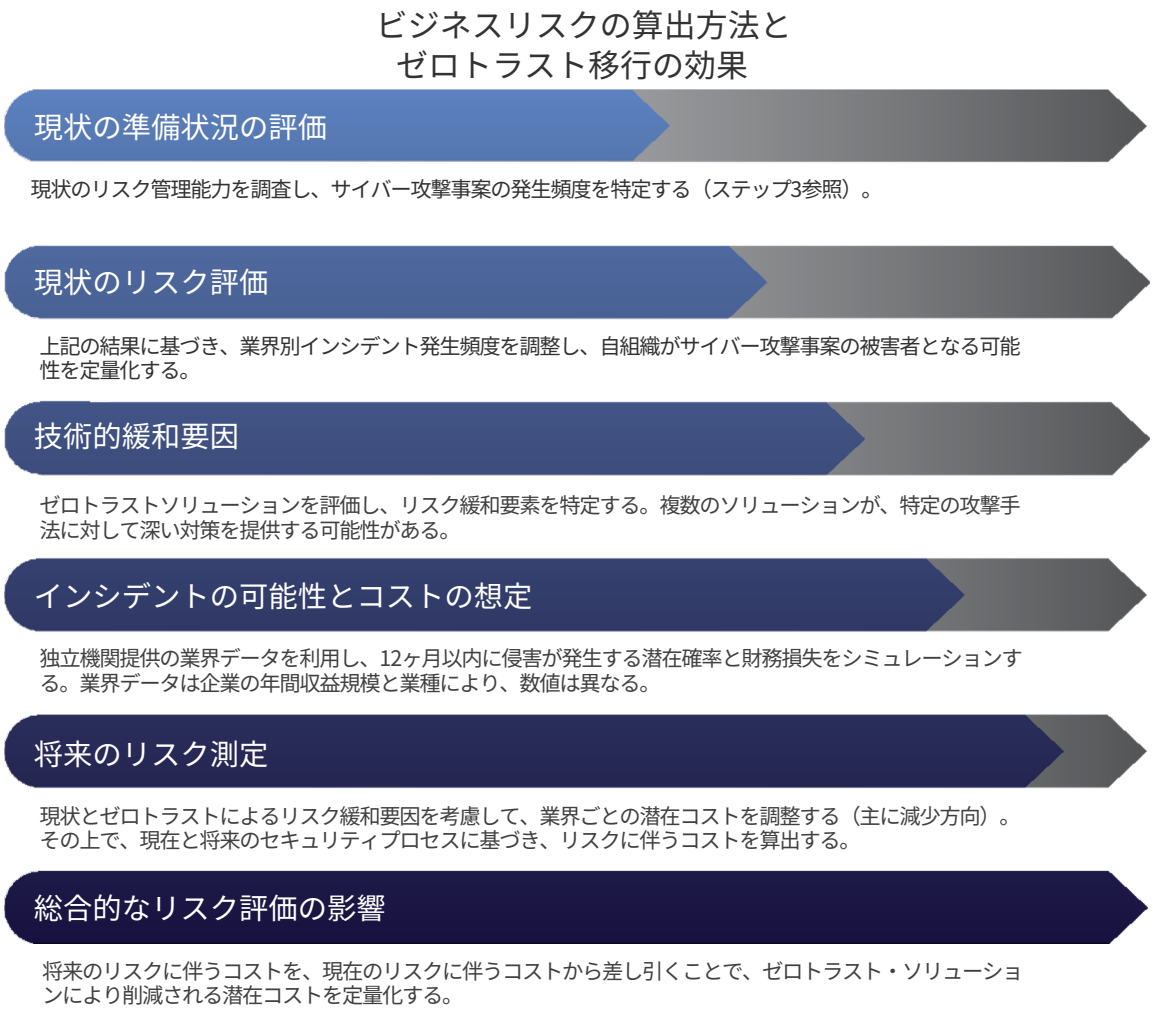


図30： ゼロトラスト・セキュリティの財務上のプラス効果を計算するためのガイドライン

ゼロトラストによるリスク低減の例

ある多国籍医療プロバイダーは、準備状況評価によって、現在のセキュリティ適用範囲が平均的であると判定されました（レガシーアーキテクチャーに基づく）。その場合、業界データによると、12カ月以内にサイバー攻撃を受ける確率は33%でした。また、シミュレーション分析では、潜在的な損失は240万ドルと推定されましたが、ゼロトラストを採用することで、これを36万ドルまで減らすことができました。この結果、この顧客は200万ドル以上の潜在的リスクを軽減することができました。

ここで概説した戦略は一挙に実行できるものではないため、サイバーリスク軽減を継続的な取り組みとして捉えることが重要です。

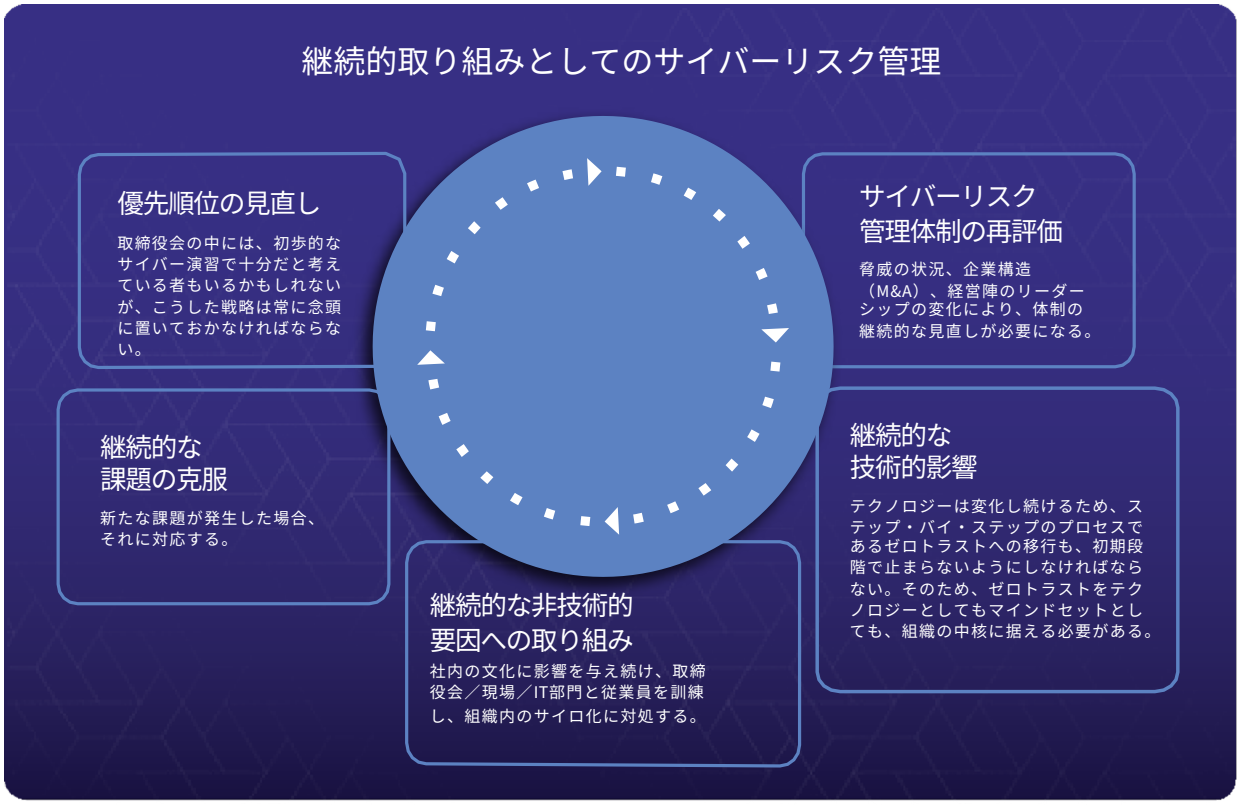
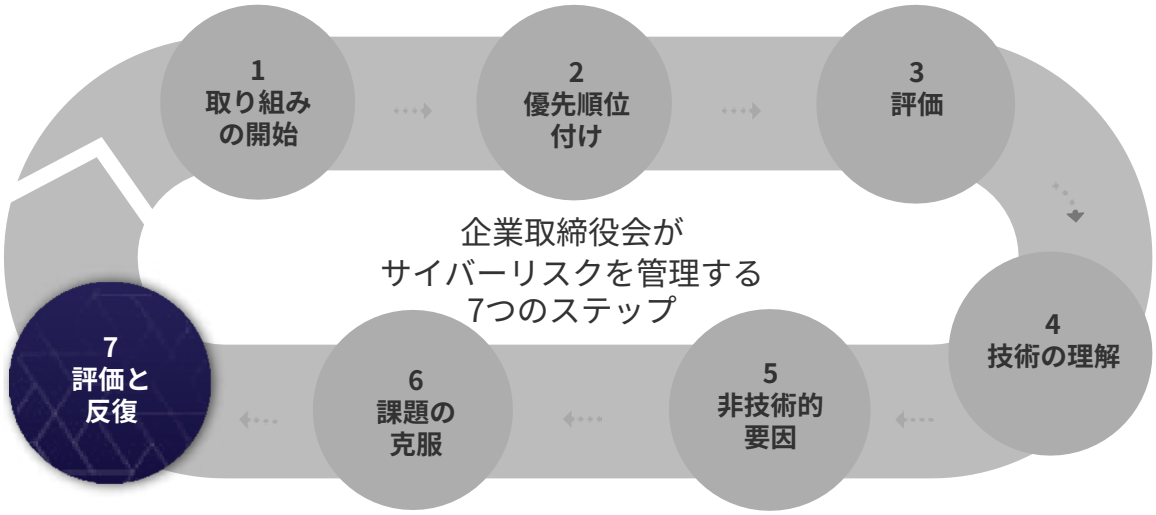


図31： サイバーリスク管理は継続的な取り組みである。

キーポイント



- 組織は継続的にリスク評価を実施し、組織が変化すると共に進化する脅威を特定し、リスクの進化を以前の評価と比較する必要がある。
- 組織は、リスク削減、コスト削減、業務効率化を通じて、ゼロトラスト移行のメリットを定量化することができる。侵害の防止によって回避されるコストの推定額は、取締役会が把握すべき重要な指標となる。
- 取締役会は、サイバー攻撃事案の発生可能性、金銭的な損失、ゼロトラストによるリスク低減に基づくシミュレーションを使用して、サイバーリスクの財務的影響を算出したデータを提供するよう求めるべきである。
- 取締役会は、サイバー戦略の再優先順位付け、リスク管理体制の再評価を奨励し、テクノロジーや組織文化全体におけるサイバーの重要性に継続的に影響を与え、新たな課題への適応能力を向上させるよう努めるべきである。
- サイバーリスク管理は、組織にとって継続的なプロセスであり、ゼロトラストへの取り組みの評価、実施、測定を繰り返す必要がある。

サイバーリスク管理チェックリスト

取締役と経営陣は協力して、以下のことに取り組む必要があります:

Step 1 - 取り組みの開始

- ☐ 組織の技術的ケイパビリティとプロセスを理解する
- ☐ 組織のサイバーリスクに対する脆弱性を評価する
- ☐ より広範なリスク課題の一部としてサイバーセキュリティに焦点を当てる

Step 2 - 優先順位付け

- ☐ サイバー攻撃に関する一般的な理解を深める
- ☐ サイバーリスクが財務的安定性をどのように脅かすかを理解する
- ☐ サイバーリスクが現在進行形で増大しつつある危険であることを理解する

Step 3 - 評価

- ☐ 侵害されやすさを評価する
- ☐ サイバー準備体制と成熟度レベルを確認する
- ☐ サイバーリスク評価と金銭的影響の分析を組み合わせる

Step 4 - 技術の理解

- ☐ 優先して保護すべき資産を決定する
- ☐ 既存のアーキテクチャーの問題点を理解する
- ☐ ゼロトラスト・アーキテクチャーの採用

Step 5 – 非技術的要因への取り組み

- ☐ 組織文化とマインドセットを考慮する
- ☐ セキュリティプロセスを最適化し、ITサイロを最小化する
- ☐ 従業員のスキルセットを適応させる

Step 6 – 課題の克服

- ☐ 取締役会のサイバー専門知識不足への対応
- ☐ 複雑なサイバー脅威の状況を理解する
- ☐ 組織のリスク状況の可視化

Step 7 – 評価と反復

- ☐ リスク削減のメリットを定量化
- ☐ サイバーリスクの金銭的影響の算定
- ☐ サイバー体制の継続的な再評価と改善

用語集

受容可能なリスク - 組織が望ましい結果を得るために許容できるリスクのレベル。
攻撃対象領域 - 攻撃者がシステムに侵入し、影響を与え、データを奪おうとするポイント。
ビーチヘッド - 攻撃者がシステムへのさらなる攻撃を開始するために使用する最初のアクセスポイント。
城と堀のセキュリティ - 周囲の防御に重点を置きながら、その防御の内側のすべてを暗黙のうちに信頼するアプローチ。
CISA - 米国の政府機関であるサイバーセキュリティ・インフラストラクチャ・セキュリティ局（Cybersecurity and Infrastructure Security Agency）。
危殆化 - ユーザー認証情報を盗むなど、攻撃者がシステムの一部に侵入すること。
企業ネットワーク - 組織のシステムとデータの相互接続性。
サイバー攻撃 - 不正なシステムアクセス、データ破壊、窃盗、改ざん、サービス拒否によって組織に悪影響を与える事象。
サイバー統制 - サイバー強靭性の目標を達成するための技術を適用する統制。
サイバーリスクフレームワーク - 標準、ガイドライン、ベストプラクティスを適用してサイバーリスクを管理するアプローチ。
サイバーセキュリティ - サイバー攻撃からの保護。
サイバー脅威 - 情報システムを通じて組織に悪影響を及ぼす可能性のあるあらゆる状況または事象。
データ - 人間または機械による通信、解釈、処理に適した情報。
データ漏洩 - 機密情報への不正アクセスや盗難。
データ損失 - 盗難や漏洩によって機密情報、専有情報、機密情報が暴露されること。
復号化 - 暗号化されたデータを読み取り可能な形式に復号化すること。
事業分割 - 企業の資産や事業の一部を売却すること。

暗号化 - データを暗号化し、許可された関係者だけがアクセスできるようにすること。

大統領令14028 - バイデン政権が2021年に発表した国家のサイバーセキュリティの改善に関する米国大統領令。

エクスプロイト - 悪意のある目的のために脆弱性を利用すること。

外部攻撃対象領域 -攻撃者がシステムにアクセスする足掛かりとなる、一般にアクセス可能な脆弱性。

ハブ・アンド・スポーク型ネットワーク - すべてが中央のデータセンターを通じて接続されるネットワーク・トポロジー。

IaaS - Infrastructure as a Service、AWSやAzureのようなクラウド・プロバイダー。

暗黙の信頼型アーキテクチャー - ネットワークに接続するすべてのものがデフォルトで信頼されていると仮定するネットワーク・モデル。

内部脅威 - 組織内部の人間によって引き起こされるデータ侵害。

IoT/OTシステム -工場設備のような、モノのインターネット（Internet of Things）と運用技術（Operational Technology）。

水平方向への移動 - 最初のアクセスを獲得した後、ネットワーク上をチェックされずに移動する能力。

最小特権 - タスクを達成するために必要な最小限のアクセスを許可すること。

多要素認証（MFA） - バイオメトリクスのような複数の形式の本人確認を要求すること。

国家アクター - 政府機関がスポンサーとなっている攻撃者グループ。ネットワーク・セグメンテーション - セキュリティを強化するためにネットワークを分割する技術。

Never trust, always verify（決して信頼せず、常に管理せよ） - デフォルトですべてのアクセスを拒否し、アクセスを許可する前に各リクエストを検証すること。

NIST -米国政府機関である米国立標準技術研究所（National Institute of Standards and Technology）。800-207は、ゼロトラスト原則の中核となる要素を示した一連のサイバーセキュリティ対策とガイドラインである。

フィッシング - 信頼できる送信元を装った詐欺的な電子メールや通信。

プライベート・アプリケーション - 組織内部でホストされ、管理されるソフトウェアリソース。

パブリック・アプリケーション - 外部でホストされる、サービスとしてのソフトウェアアプリケーション。

ランサムウェア - 身代金を支払うまでデータを暗号化する悪意のあるソフトウェア。

リスク軽減 - 予防措置や管理策を講じることでサイバーリスクを低減すること。

リスク管理体制（リスクポスチャ） - リスクを発見、認識、説明するプロセス。

リスク転嫁 - サイバー保険などを通じてサイバーリスクを別の当事者に転嫁すること。

SaaS - サービスとしてのソフトウェア、クラウドでホストされるアプリケーション。

技術的負債 - 時代遅れの技術や安全でない技術を修復するためのコスト。

サードパーティ - ベンダー、パートナー企業、サービスプロバイダーなどの外部エンティティ。

脅威行為者 - システムの侵害や攻撃を試みる個人。

トランザクション - ファイルやアプリケーションへのアクセスなど、個別のやり取り。

トラバーサブルスペース - リソースにオープンにアクセスできるネットワークアーキテクチャー。

TSA - 資産売却時に一時的なサービスを提供するための移行サービス契約。

ユーザー認証 - ユーザー、プロセス、またはデバイスの身元を確認すること。

仮想プライベートネットワーク（VPN） - 企業リソースへの安全なリモート・アクセスのための暗号化トンネル。

脆弱性 - 攻撃者に悪用される可能性のある欠陥や設定ミス。

ゼロトラストアーキテクチャー（ZTA） - 各リクエストを検証し、最小特権アクセスを許可することで、暗黙の信頼を排除するモデル。

Zscalerについて

Zscaler (NASDAQ: ZS) はデジタルトランスフォーメーションを加速させ、顧客企業における俊敏性、効率性、弾力性、安全を強化します。Zscaler Zero Trust Exchange™ プラットフォームは、あらゆる場所に存在するユーザー、デバイス、アプリケーションを安全に接続することで、何千もの顧客をサイバー攻撃やデータ損失から守ります。世界中の150以上のデータセンターに分散されたSSEベースのZero Trust Exchange™は、世界最大のインラインクラウド・セキュリティプラットフォームです。

今日、そして明日を変革する

地球上で最大のセキュリティクラウドを活用することで、Zscalerは世界の一流企業のビジネスを予測し、保護し、簡素化しています。

セキュアなデジタルトランスフォーメーション

Zscalerは、デジタルトランスフォーメーションを加速することで、顧客企業がより俊敏、効率的で、弾力性があり、セキュアであることを可能にします。クラウドネイティブのZero Trust Exchangeプラットフォームは、あらゆる場所にいるユーザー、デバイス、アプリケーションを安全に接続することで、何千ものお客様をサイバー攻撃やデータ損失から守ります。

2007年の創業以来、驚異的な成長を遂げてきたZscalerは、常に安全かつシームレスに情報のやり取りができる世界を実現するために存在しています。Zscalerの使命は、ビジネスを予測し、安全にし、簡素化することで、今日と明日を変革することです。

数字で見るZscaler

#1 ガートナーMQリーダー、SSE実行能力で首位	**74** ネットプロモータースコア（SaaS企業平均は30）	**250+** 発行済みまたは出願中の特許数	**40%** Fortune 500企業での採用割合
150 ゼロトラストエクスチェンジの数	**300B+** リクエスト数/日	**7B+** 阻止されたインシデント数/日	**7K+** 顧客企業数

セキュリティとは脅威からの保護以上のものである

クラウドリソースへの高速かつ安全なアクセスは、今日のクラウドファーストの世界における変革の重要な推進力です。Zscalerは、ゼロトラストの原則に基づき、IT部門がレガシーなネットワークインフラから脱却し、モダンワークプレイスの実現、インフラの近代化、セキュリティの変革を達成できるよう支援します。

- **モダンワークプレイスの実現** -従業員、パートナー企業、顧客企業、サプライヤーに、場所やデバイスを問わずアプリケーションに安全にアクセスできる環境を提供し、常に優れたデジタル体験を実現します。
- **インフラストラクチャの刷新** - ゼロトラスト・コネクティビティ、セグメンテーション、ポスチャコントロールにより、クラウドワークロードとクラウド/SaaSデータを保護します。
- **セキュリティトランスフォーメーション** - IoTおよびOTデバイスにゼロトラストのインターネットアクセスを、OTデバイスに特権的リモートアクセスを提供します。
- **脅威を止め、イノベーションを始める** -セキュリティとは、より包括的で、つながりのある、エンパワーメントされた世界の基盤であるとZscalerは考えています。

お客様のビジネス体験における予測、安全の確保、簡素化を支援することで、能力、専門知識、洞察力が活かされ、今日の最も優れたアイデアが明日の最も革新的なイノベーションとなることを支援します。

さらに詳しく知る

取締役会の一員として、効果的なサイバーリスク管理を行うために必要な知識を身につけることができたかと思います。本書でご紹介しているステップは、現代のデジタル社会がもたらす課題を乗り切るための道筋を示すものです。

さらなる情報を得るには、以下のリソースをご活用ください：

CXO REvolutionaries

CXOによりCXOのために作成されました。世界の大企業にクラウド＆モバイルファーストの新潮流をもたらすITリーダーから学びましょう。デジタルトランスフォーメーションのパイオニアや、ソートリーダーによる最新の知見を掲載しています。

Zscaler.com

Zero Trust Exchangeプラットフォームの開発元であるZscalerは、地球上で最大のセキュリティクラウドを使用して、ビジネスを行い、変化をナビゲートすることで、よりシンプルで迅速かつ生産的な体験を提供します。

Seven Elements of Highly Successful Zero Trust Architecture eBook

Zscaler Zero Trust Exchangeに関するアーキテクト向けガイド

The 7 Pitfalls to Avoid When Selecting an SSE Solution eBook

ゼロトラストを基盤としてSSEを構築するためのヒント

Seven Questions Every CXO Must Ask About Zero Trust

セキュアデジタルトランスフォーメーションとゼロトラストに関するエグゼクティブ向けガイド

Run an Attack Surface Report for Your Domain

経営幹部の皆様の声

“すべての取締役会役員のための優れた基礎資料として本書をお勧めします。本書は、サイバーセキュリティというトピックの広範さと、それがあらゆる企業のビジネスやリスクのさまざまな側面といかに密接に結びついているかを捉えており、わかりやすく実用的な内容になっています。”

Joanna Burkey / HP INC. CISO, OVERSTOCKおよびRELIABILITYFIRST CORPディレクター

“全体を通して 素晴らしい内容です。サイバーセキュリティの問題を素晴らしい方法でフレームワーク化しています。”

Karen Blasing / AUTODESK、GITLAB、ZSCALER 取締役

“もしあなたが取締役会の一員で、サイバーセキュリティの学習曲線を素早く登ろうとしているならば、本書でサイバーリスクの効果的な管理・軽減の実現に必要な重要なステップを短時間で学ぶ事ができます。”

Eric Spiegel /取締役およびシニア・アドバイザー

“今後10年間でテクノロジーとデジタルトランスフォーメーションの影響が増大する中、企業にとっての最大のリスクのひとつは、サイバーセキュリティの脅威の増大です。この重要な管理の役割を会議室のテクノロジー専門家に任せるだけでは不十分です。すべての取締役にとって、この7ステップガイドは、実践的かつ包括的なフレームワークとして役立ちます。リスクを軽減し、組織としての備えを確実にするためのフレームワークです。”

Anna C. Catalano /取締役会ディレクター

“サイバーは、すべての組織にとって深刻化しているリスクです。あらゆる役員会議に専門知識を導入し、組織文化とゼロトラスト環境を監督して、重大な情報漏洩の可能性を軽減することが極めて重要です。『サイバーセキュリティ 取締役会のための7つのステップ』は、この問題について考え始めるのに最適なきっかけです。”

Catherine Lego / GUIDEWIRE、CIRRUS LOGIC 取締役